AI4D - Digital and Biometric Identity Systems

Gabriella Razzano

RESEARCH ICT AFRICA
IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international
Canada
Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY
AI4DAFRICA

Table of Contents

Executive Summary

This policy paper examines issues emerging around the deployment of Artificial Intelligence (AI) in Digital and Biometric Identities (BDI) being rolled out across Africa as a central part of digital strategies to meet the UN 2030 Sustainable Development Goals (SDGs).

SDGs Target 16.9 aims: "to provide legal identity for all, including birth registration by the year 2030". Digital identity is also seen as key to unlocking various other development goals including universal health and education access, and financial inclusion. BDI systems present opportunities for enhancing the visibility of benefectors of social services, enhancing efficiencies in digital transacting, and a variety of other potential social and digital economy benefits.

The literature demonstrates that emergences of AI in the BDI context, however, exacerbate risks already present to both fields that arise from the centrality of personal data, mass collected and analysed, within their systems. And there are broader risks – some of which arise from the centrality of identity, some of which arise from the nature of AI, and some due to the combination of both. These include for instance, exclusion from systems due to bias or inefficiencies; lack of accountability given stakeholder relationships and the nature of the technologies themselves; heightened risks for surveillance or monitoring; improper delegation of functions; and different ramifications of technology dependencies. These challenges might be directly addressed by different forms of policy solutions, which specifically advance forms of transparency mechanism, human rights and other legal instruments, and/or design solutions.

This paper draws on two cases studies – one in Ghana involving facial recognition software, and another in South Africa involving natural language processing – to add depth to these background findings on the complexities of BDI systems and AI in Africa. Within conversations on BDI, there are two key forms of digital identity: foundational digital identity is associated with foundational public sector functions, such as national and civil registration systems, whilst functional digital identity systems are those decentralised identity systems for specific sectors or use cases (Bhandari et al., 2020). Both case studies emerge as largely functional examples of digital identity projects, with only tangential relationships to foundational identity systems. This divergence, however, is an important finding for considering the potential environment in which the AI aspects of BDI will emerge.

In Ghana, BACE-API has been launched as a form of facial recognition technology specifically trained to identify African faces. The case study demonstrates that, though the technology is framed as having development goals, the ability of the technology to combat financial exclusion is questionable – since it does not seek to deal with the structural impediment underpinning that exclusion. Additionally, the challenges in opacity within private sector interventions make it immensely challenging to identify specific harms and mitigate risks. African solutions to African problems will first have to deal with the challenges within the innovation environment, variability in the policy and regulatory environment, and then directly tackle the digital inequalities that mark that context. Exploring a strong business case on top of those preliminary hurdles then becomes the goal for intiatives like BACE-API.

In South Africa, GovChat (also a private sector company) has been launched largely as a communciations platform for connecting government and citizens. Apparently enhanced by natural language processing AI, one iteration of the product collects identity information for helping to process social distress-relief grants. It does not collect biometric data, but does collect national identity numbers. Nevertheless, the historical context applicable to the case study on biometric data and foundational identity has helped unpack dimensions of opportunities and risks within the AI and

data environment. Like Ghana, this project was more reflection of functional identity than foundational identity, but demonstrated some of challenges in trying to create pivoting business models in a context of high risk personal data. Importantly too, competition-related disputes between GovChat and WhatsApp provide a vital highglight of how competiton regulation – and its domestic enforcement – might play out as a tool for combatting the global technological domination of certain firms.

While the actual use of AI technologies may not be particularly advanced in the BDI context, there are historical lessons to be considered for future policy interventions for the African region, with social, political, and historical aspects of identity being central to understanding the technological dimensions of AI. Both case studies, importantly, demonstrate how a consideration of incentives across these dimensions inform policy choices; and how alternative incentives are necessary if different outcomes are desired.

The comparison of the case studies provide insight across themes relating to global governance; digital hegemonies and public-private intersections; foundational digital identity; the digital economy and innovation environments; AI and its role in relation to visibility; the centrality and importance of transparency; and strategies for addressing risks.

These case studies thus result in the following recommendations:

For Future Research

- In terms of broader future research, the case studies raise the importance of creating a research framework or methodology for helping to define how functional and foundational do and do not correspond.
- In terms of future case studies in this area, significant energy should be placed on outlining the actual data processing practices that underscore biometric and digital identity technologies.
- In terms of policy intervention areas, guidelines for the institution of socio-economic risk assessments of biometric and digital identity projects should be outlined.
- Identity projects arise within a particular social and political history of exclusion for many African populations. This will need to influence what we consider useful interventions to be, but also means it will be a reality that a significant area of AI technology will relate to identity authentication processes in the near future. Creating norms and standards for these kinds of activities should be a research priority.
- As more AI technologies are developed, a strong focus in the research should be considering the specific *type* of AI technologies being implemented and the specific *types* of data underpinning it – risk assessments should be technologically specific.

For Policymakers

- Data governance frameworks are a priority foundation for the implementation of biometric and digital identity programmes.
- Foundational identity projects will need to constructively coalesce with functional identities in order to reap the benefits of good AI.
- All policies must be established within a considered analysis of the full extent of intersecting digital inequalities.

For Lawmakers

- Regulatory interventions should consider the extension of transparency mechanisms in the context of biometric and digital identity, in particular.
- The expansion of social obligations for assuring good AI must be assured given the role of the private sector in the delivery of public goods and services.

For Technologists

- The implementation of socially focused identity projects should remain authentically connected to their public good purpose.
- Socio-economic risk assessments should be implemented prior to, and post, the implementation of biometric and digital identity AI technologies.

Part A: Introduction

1. Project Background

The Mapping AI for Development in Africa (AI4D) project is a response to the research agenda for the ethical and equitable application of Artificial Intelligence (AI) in the Global South proposed in the IDRC whitepaper, "Artificial Intelligence and Human Development". The project conducted case studies on AI deployment across the African continent and the associated policy and governance implications. It explored AI in relation to four thematic areas – biometric identity, computer vision and surveillance, skills capacity and workforce development, and gender. This report covers the Digital and Biometric Identity (BDI) theme. Research for each thematic area began with a broad mapping exercise to search for examples of AI initiatives across Africa, followed by deeper analysis of a selection of the identified examples. The themes were examined in terms of the potential contribution of AI systems to public service delivery specifically and socio-economic development generally, the challenges AI systems present for African countries, and the role of both public and private sector actors.

In the context of Research ICT Africa's (RIA's) ongoing work on digital and social inequalities, the research was framed by concerns about whether the appropriate systems and mechanisms are in place to deliver benefits and safeguard against the harms and risks associated with AI, especially for the most marginalized populations. The potential positive impacts of AI technologies were examined against the social, economic, political, and historical realities within case study countries and in global context; with particular attention to the interplay amongst the state, markets, and citizens in the delivery of public services, especially those that are partially or fully provided by private sector actors. Social justice and human rights lenses were applied to reflect on the legal and ethical frameworks required to safeguard human rights and ensure data and privacy protection as well as data justice. These perspectives feed into recommendations for the design of policies that enable beneficial, inclusive, and rights-based AI in Africa.

2. Artificial Intelligence and Development

AI moves beyond just automated decision-making and algorithms, to include concepts on machine learning. Big data and algorithmic decision-making may be included under a broader AI rubric, in which case its useful to understand algorithms as a "set of instructions" that are created, and given, through design – more so in rules-based systems than machine learning systems (Hong Chang & Kuen, 2019). However, a definition can be provided, which sees AI as computer programmes that mimic human intelligence and cognition (human intelligence being understood as reasoning, learning and problem-solving) (Marwala, 2015; PricewaterhouseCoopers, 2018).

There is significant potential for AI to directly contribute to improving public service delivery, by helping to address long-standing public service challenges "… such as high turnover rates, large unmanageable caseloads, administrative burdens, long waiting times, and delays in service delivery and language barriers" (Wirtz & Weyerer, 2019). These forms of AI for enhancing efficiencies, though, stand as a lower order imaging of AI benefits (Stahl, 2021). Human flourishing and development objectives, should focus public sector design and implementation of AI (Stahl, 2021). Of course, equating public sector AI use with development outcomes is not sufficient. Development outcomes might be influenced by the private sector, or through public-private partnerships (Razzano, 2020c). However, the development objectives on incorporated AI must be considered within the context of

specific AI risks (Creese, 2020). Of particular concern is the way AI might contribute to uneven development.

3. Digital and Biometric Identity

3.1 Introduction

Within conversations on BDI, there are two key forms of digital identity itself: foundational digital identity is digital identity associated to foundational public sector functions, which would include national and civil registration systems (Bhandari et al., 2020). In contrast, functional digital identity systems are those decentralised identity systems for specific sectors or use cases (Bhandari et al., 2020).

Biometric identities are not equitable to digital identity but are a form of digital identity system that identifies through biometric markers. Digital identity can more broadly be based upon any number of personal identity markers. Thus, central to both biometric and digital identity systems is *personal* data of the nature generally subject to specific data protection regulations.

Generally, biometric identity is intended for one-to-one identity verification. In other words, your biometric information is compared to an electronic digital template on the database in question (Privacy International, 2013). However, there are also one-to-many systems, which are often the more significant threats to privacy (Privacy International, 2013), i.e. systems that take an unknown person and run them against a database containing a mass of biometric information of known persons.

BDI has different intersections with AI systems. The pure identification function, after all, is largely a database-centred function. However, algorithmic decision-making will likely be used to process the data contained within those systems and can be used within the verification process (Matthers, 2019). In relation to more extended connections to machine learning, such learning might be used to process large data sets with unlabelled data points to ensure, or at least approximate, user identity (Qorbani, 2017).

A biometric or digital identity system may employ AI. In turn, both biometric identity systems and AI systems are predicated on the collection and processing of personal and other forms of data.

3.2 History

When we focus on the technological aspects of either AI or BDI, these seem like new phenomena. However, digital identity systems have been a central organising system for civic life for many years. Fingerprints were used in the context of identity verification in China in the 14th Century (Privacy International, 2013). And, as the case studies demonstrate, biometrics have been incorporated within identity systems in certain regional countries for many decades. For instance in South Africa, biometric data collection was almost always a part of traditional social grant verification, with biometric fingerprinting being used by colonial and apartheid administrations (Donovan, 2015; Vally, 2016).

These historical foundations are incredibly important for understanding the role of BDI within its regional context (and there is a significant body of literature available on the socio-historical and political dimensions of identity). Its foundational function is classification of persons for access (to services, etc.) – thus exclusion too is a foundational challenge.

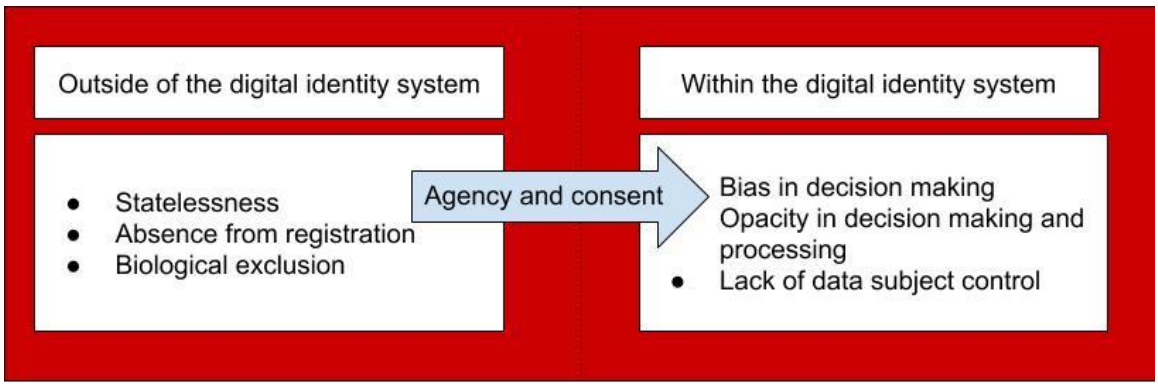


Figure 1: Patterns of exclusion and risks © Razzano 2020

3.3 Overarching risks and harms

Data protections

There are a significant number of concerns that arise directly from BDI systems and their reliance on personal data. In fact, fuelled by the AI 'wave' and growing demands for big data, there is both a private and public sector-led tendency to mass data collection. Ambitions for comprehensive digital identity systems have been influenced by the foundational work of multilateral organisations like the World Bank and International Monetary Fund (Razzano, 2020a; World Bank, 2019). The GSMA has a specific Digital Identity Programme focused on mobile technologies (GSMA, 2019).

It is important when examining BDI systems to include a data protection frame. Data protection is underscored by an emerging normative framework for assessing the protection and processing of personal data, in particular. These processing principles include:

- collection limitation;
- purpose specification;
- use limitation;
- data quality;
- security safeguards;
- openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives), and
- accountability (Razzano, Gillwald, et al., 2020).

BDI systems rely on data collection, but the retention of the data increases the risks and threats associated with processing (Razzano, 2020; World Bank, 2019). The ideas around collection and retention also highlight how data security must be imperative. Cautionary tales about biometric systems relate strongly to the data protection element in part because there are emerging standards for considering it, but also because of the very real threats that might arise in jurisdictions that do not have data protection frameworks in place (such as the UNCHR's refugee processing programmes) (Privacy International, 2013). Who has access to the databases underscoring BDI systems is an important consideration, too, for limiting the associated security (and other) data risks – for example, a key challenge to the Mongolian BDI system was the number of agencies that were permitted direct access (Bhandari et al., 2020; Privacy International, 2013).

The limitation of processing personal data within BDI systems for their original purpose is a necessity to avoid risks to data subjects (Reed & Ng, 2019). By overly defining the purpose, you increase the potential not only for abuses, but for increasing the number of persons who might access a data set. This is why an essential aspect of *good* data practice is ensuring data minimisation (Razzano, 2020a).

Importantly within the BDI environment, however, is the issue that a central tenet to much of data protection paradigms is the notion of consent by subjects to have their data processed. Given the verification purposes of BDI systems largely for forms of benefit, this raises incredibly important caveats for considering whether such concepts provide any realistic protection in this context (Razzano, 2020b).

Data protection frames itself as processing limitations in order to help protect against privacy harms such as fraud and the misuse of data. This is because, even prior to a harm being experienced, once data is 'breached' the *potential* for harm is essentially irreversible (Privacy International, 2013).

Exclusion

The associated risk of exclusion is a fundamentally important one for considering BDI systems (as reflected on under the historical context). For many, there is a very direct benefit to being visible to the state: for instance, for the receipt of life-sustaining grants requiring digital identity verification (Srinivasan et al., 2018). One of the most significant barriers to accessing grants historically has been a lack of identity documents; for many citizens, you are not a 'person' to the state unless you are a 'number' too (Srinivasan et al., 2018). For refugees, it may mean fundamental protections and resources being provided to them through the UNHRC's Refugee Programme. This has a very real impact on the ability of persons to 'consent' to the processing of their data (Razzano, 2021).

The systems themselves might also result in unfair exclusion. In biometric verification processes, false negatives and false positives happen: while iris recognition is the most accurate, facial and fingerprint reliability is less so (Privacy International, 2013). In relation to biometric data reliability itself, there may even be biological impediments to persons inclusion in a system (such as a labourers with worn fingerprints) (Privacy International, 2013). Cultural norms may also result in unfair exclusions from BDI systems that require biometric data for inclusion (Privacy International, 2013).

However, this also means that algorithmic decision making that relates to such systems, and their associated bias and exclusion challenges, are an immense concern. Examples of algorithmic bias and its impacts on criminal reoffending are such an example (Hong Chang & Kuen, 2019). The sources of algorithmic bias is complicated (Hao, n.d.). Much of the bias might be inherent to the data itself. So, for example, the dataset underpinning the process may be skewed, or the algorithm may be looking for unfair data points, but the result is nevertheless a disproportionate (and inaccurate) response to a particular grouping (Srinivasan et al., 2018). Not least of all this means that the systems themselves must collect reliable and credible data, implicating data governance practices (Reed & Ng, 2019). BDI systems that use algorithms for verification therefore also bear these risks for exclusion.

Accountability

BDI systems may centralise data collection in the hands of agencies over which there is little oversight, such as in security agencies (Privacy International, 2013). The accountability challenges extend not just to the data collection and retention itself, but also to algorithms making verification (or other BDI necessity based) decisions. Explainability of the algorithms can be a challenge, either intentionally, intrinsically or technically (Cobbe, 2018). This means the ability for recourse is limited, but so too is the ability to properly assess such systems for *potential* risks (Crawford & Calo, 2016).

Improper delegation

If decisions are made by algorithms within, or related to, BDI systems, within the administrative justice sector this may constitute an improper delegation of authority (Cobbe, 2018). Some data protection frameworks in fact prohibit, or limit automated, decision-making based on personal data. When institutions devolve themselves of their decision-making powers, the onus of proving, or disproving, why a citizen *should* be included within or by a BDI system is unfairly shifted to the citizen (Hong Chang & Kuen, 2019).

Surveillance

Concerns in relation to associations between BDI systems and surveillance arise when we move from one-to-one systems, to one-to-many systems (Privacy International, 2013). The incredible expanse of digital identity systems (as addressed above) significantly increases the risk of abuses of data, with unjustifiable surveillance being a key concern for many, particularly in the region. AI greatly enhances the powers for surveillance and biometric data (as the source of data underscoring BDI systems) makes it both more accurate and more invasive than ordinary surveillance – famously, the Zimbabwean government traded citizen biometric data (in the form of facial data) collected as part of its public mandate to Chinese companies for the use of facial recognition software domestically (Besaw & Filitz, 2019).

This is a specific kind of privacy risk worth mentioning – the increased risk of 'dataveillance' from the state (Privacy International, 2013), but also the increased exploitation of data from the private sector in the pursuit of 'surveillance capitalism' (Zuboff, 2018). When both holders of power (coercive and economic) are pursuing the same thing – big data embedded with personal markers - the opportunities for collusion and abuse expound. It should be remembered that underscoring any state data collection project is the potential incentive of social control through identification and classification of citizens (Gangadharan, 2017; Suchman et al., 2017).

Technology reliance

There are also challenges that relate directly to the introduction of new technologies within the digital identity system process. In developing countries were electricity supply may be unstable, this means essential BDI systems may go offline: the Kenya elections were in fact threatened by the introduction of new electoral systems that struggled with both electricity supply and Internet coverage, meaning a manual back up is relied on (Privacy International, 2013). With Internet penetration still a challenge across the continent, particularly in rural areas, new forms of digital exclusion emerge, which relate to the provision of state services that begin to be associated to new BDI systems. Additionally, insufficient public sector capacity, which may lead to dependence on external resources but also proprietal technologies, brings with it significant risks of "vendor lock-in" that undermine economic efficiencies in public service delivery (Breckenridge, 2019).

3.4 Overarching policy solutions

Transparency

Transparency is an essential counter to many of the challenges and risks associated to BDI systems. There are transparency challenges that relate to the systems themselves: the contracts and associated documents that underscore the private/public partnerships at the centre of the many of these initiatives must be available for scrutiny. This public/private intersection also speaks to the necessity for transparent and fair procurement systems.

In the data processing aspects of BDI systems, whether or not algorithms used are rules-based automation or more related to the 'black box' of machine learning, becomes a challenge in trying to ensure transparency in relation to the *decision-making* process itself (Hong Chang & Kuen, 2019). Nevertheless, explainability impacts your ability to challenge decisions (which might include either inclusion or exclusion from a BDI-based system) (Barocas & Nissenbaum, 2013; Pasquale, 2015). There are two key types of explainability 'rights': rights to understanding the specific decisions taken (Wachter & Mittelstadt, 2018), which is more similar to administrative decisions, versus a right to system functionality explanations. In situations where the mechanics of the explanation may be difficult, the onus then shifts to accountability – who is ultimately responsible for explaining the decision, if it has negative impacts (Hong Chang & Kuen, 2019)? In such a situation, traditional ideas developing from administrative justice can again be instructive. And there is a very interesting form of Algorithmic Impact Assessment that acts as a form of classification or 'triage,' developed by the Canadian Treasury Board Directive on Automated Decision-making that could be referenced, for helping to determine how the development of a system should take place (Hong Chang & Kuen, 2019).

As noted, many data protection frameworks (such as the EU General Data Protection Regulations or South Africa's Protection of Personal Information Act) provide forms of blanket exclusions on automated decision-making based on personal data, but it will be worthwhile monitoring how the decisions relating to such clauses develop.

Human rights frameworks

Human rights frameworks give an important normative framework for understanding challenges in the context of individual rights. It also presents an important opportunity for giving recourse in relation to BDI system challenges that might arise. When assessed against human rights standards, questions such as 'necessity' (which was raised as a key concern in relation to the Israeli BDI database) become centralised as measures for controlling risks (Barocas & Nissenbaum, 2013; Pasquale, 2015). Legality, necessity and proportionality become part of an important test for determining whether or not a BDI system unjustifiably limits the rights of citizens that may, or may not, be subject to it (Bhandari et al., 2020).

Other existing legal mechanisms (sectoral laws)

As an important extension of the principle of legality, there may be sectoral or other laws within countries (rather than extra-judicially where international law principles provide guidance) that further constrain BDI systems. As seen before, for decisions from the public sector based on BDI system algorithms, automated decisions might be subject to administrative justice principles (Cobbe, 2018).

In turn, the data that underscores such systems might be implicated for processing in terms of relevant data protection law systems where they exist.

Design

Direct solutions can be embedded into the design of the BDI systems themselves, presuming they are at a stage that could allow for mitigating against a particular harm still (Baker, 2019). Privacy by design solutions should ensure that the physical digital structure is able to assure security (Privacy International, 2013). Equality by design solutions can also be imposed – in other words, direct technical interventions that could assist in mitigating against the inequality and exclusionary harms so far identified.

4. Application to Research Approach

4.1 BDI Specific Framework

What emerges then from the literature, if we take a data subject centred approach to the people that may be the subjects of a BDI system that in turn is based on the collection and processing of personal data, are key areas of focus for determining potential risks:

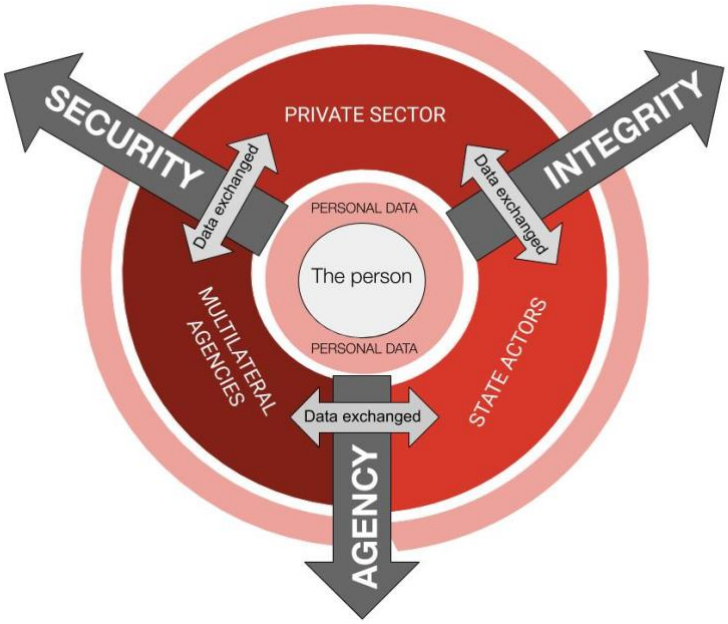


Figure 2: Modes of constructing digital identity © Razzano 2020

The diagram therefore alludes to broader data processing principles, but centred on the concerns of the subjects themselves. And of course, if challenges are identified, a further dimension then arises in relation to *accountability* and *recourse*.

The accountability and recourse dimensions also pivot us to specific concerns, which emerge from BDI systems intersections with AI – while data protection concerns are relevant to both areas, the AI and machine learning components highlight the association between BDI systems and their relation to decision-making (which surface the twin threats of bias and inadequate accountability).

When considering the intersections between AI and the different thematic areas of concern, a key distinguishing feature, which emerges to assist in ensuring that data governance questions alone are not conflated as AI concerns, is an understanding of "processing plus" – the idea that AI extends to decision-making and learning making its risks and opportunities extend beyond mere data processing challenges.

Digital inequalities must be centred for considering the African dimensions of AI and BDI systems with a focus on the specific relationship between poverty and privacy. Decyborgisation is reducing marginalized communities to a state of biological subsistence so that they are no longer political subjects, but mere inhabitants struggling for subsistence within community settings, as a result of differential access (Gurumurthy & Chami, 2019; Sen, 2005). Within BDI systems, the particular nuances to experienced digital inequalities concern a focus on both *exclusion* and *agency*. This is particularly because of the relationship between BDI systems and both visibility and classification.

Importantly, this digital inequality focus also means that an important component of analysis should be a focus away from technological determinism (Gandy, 2005). This should extend too to data determinism i.e., a presumption that the big data collection (or extraction) is a necessity. Human rights standards around data minimisation and necessity are useful in this regard.

In trying to provide the development of policy solutions or strategies that relate to BDI systems from the case studies, the focus should be on:

- Combatting defined risks and harms,
- Leveraging (and adapting) existing solutions, and
- Pursuing human rights normative standards as the guiding objective.

Having human rights standards as the normative frame means leveraging existing normative frames that already intersect with social, economic and political imperatives – though acknowledging some of the limitations that surround a 'strict' human rights framework in terms of both capabilities and structuralism (Gurumurthy & Chami, 2019; Sen, 2005).

4.2 Research Questions

Thematic area research questions (fully outlined in Annexure B) were originally co-created in collaboration across themes to provide a consistent frame (see further Annexure A on Research Design and Methodology). Nevertheless, based on the above context, the explanatory research questions for the overall comparative case studies on BDI covered in this paper were simplified to chiefly focus on three key questions:

- What data governance issues underscore the reality of the case study selected?
- To what extent do the relationships between different stakeholders in the case study influence, or relate, to the particular risks and/or harms of relevance to the introduction of AI (or at least AI-related) technologies in this case study?
- What can be learned from African case studies about the future of AI policy in Africa, in relation to both Biometric and Digital Identity, and AI more broadly?

Part C: Faces and Finances in Ghana AI

5. Introduction

In 2018 in Ghana, a private sector company was launched which, using AI-enhanced facial recognition software, seeks to address identity authentication challenges for the financial sector. As a regionally developed technological product, BACE-API[1] presents an important case study in examining digital economy aspects of potentially developmental technologies.

Importantly, the BACE-API is specifically designed for the recognition of African faces. A significant critique in much of the literature on AI has been the under-representation of Black faces in datasets, which is both ethically and practically problematic, resulting in the inaccuracy of AI-driven facial recognition software results and new forms of exclusion for 'marginalised' communities (Buolamwini, 2019; Buolamwini & Gebru, 2018; Raji et al., 2020; Thorat et al., 2010). This project stands as an example of a locally driven technology seeking to address that challenge.

Yet, the project is largely disconnected from the national identity regime (though it utilises some public sector data) and stands chiefly as a functional identity system, which incorporates AI for authentication. Nevertheless, this private sector initiative intersects with both development communities, and public sector interests, providing an important context for considering the reality of the AI environment in Africa. It demonstrates how, when we foreground the realities presented by an AI case study, the political and economic realities of innovation require consideration of the social and development realities as well (both in impacts and opportunities) – and how incentives across these spheres influence the legal and policy choices that are made.

6. Defining the Case Study

6.1 Technology

BACE-API is an application programming interface (API) that uses AI-enhanced facial recognition technology to help identify individuals. The selection of facial features as the form of biometric data that would be used for authentication was a deliberate selection by the company: they have noted that the more common practice of utilising fingerprints for identification has increased costs for companies in the form of the hardware required to process such identities (Hastings-Spaine, 2021). In contrast, BACE-API is designed to use the camera on a hand-held instrument like a phone or tablet, which could be owned by the individual themselves.

It is not clear what datasets BACE-API may be using to train their AI modelling. However, the verification process of data that the product uses is:

- an image is uploaded (either an identity document or camera image of the person whose identity is being confirmed);
- the product determines if the image is alive, real and "not a robot"; and

[1] The front facing website for the company can be explored here: https://www.bacegroup.com/.

- it simultaneously extracts the data on the identity document provided and matches it with facial biometrics in an issuing authority or government department (Kolawole, 2020).

The verification against official documentation process is not easy to discern from available material, though public resources have indicated that: "In partnership with a data controller that deals with certified government-issued identity documents, BACE API has access to Ghanaian passports and other identity documents to use during its verification processes" (Royal Academy of Engineering, 2020).

6.2 Stated Purpose

The company's pitch deck, obtained from the CEO through a direct request for information, cites the existing 'problem' the product seeks to address as being:

- poor existing identity schemes in the region, which result in individual financial exclusion;
- online identity fraud and high level of cybercrime in the region, which is particularly challenging for financial institutions; and
- know-your-client (KYC) compliance being incredibly costly for businesses.

Throughout their own social media marketing and online content, they have embedded their product strongly within the cybersecurity and fintech communities.[2] And KYC is certainly a challenge for African banks, with the "last mile problem" contributing to banking exclusion of rural communities (Razzano, 2020b).

6.3 Business Model and Funding

BACE-API is a business-to-business (B2B) product, which is why as an API it is designed to integrate within existing systems (Kolawole, 2020). The Ghanaian business market is not necessarily welcoming to innovations such as this, however. There are low levels of business trust in these kinds of digital solutions, which means that trust-building with clients has had to be incorporated within the BACE-API company practice (Fintech Circle, 2020)..

The Chief Executive Officer (CEO) of the company, Charlette Nguesso, has stated:

> "On the business side, since we're doing something that is not popular in Africa and targeting financial institutions, who are careful about security, we did face a lot of challenges. Plus, we're a young start-up with young people, so it was not easy to get clients initially" (Hastings-Spaine, 2021).

But the justification for the B2B model is rooted in BACE-API's market analysis, with the oft-repeated assertion that in the Ghanaian market alone businesses spend $400 million dollars yearly to identify their customers (Salaudeen, 2020)The product is being rolled out with at least two existing bank clients (Royal Academy of Engineering, 2020). It was largely developed through seed funding, and the start-up is now expanding its client base. It resulted from an idea pursued by the current team at the Meltwater Entrepreneurial School of Technology (MEST), based in Accra (one of Africa's earliest tech incubators) (Kolawole, 2020). MEST then invested USD 100 000 into the project as part of its

[2] Some of their blog contributions are centralised at: https://medium.com/@bacehq.

incubation (Shapshak, 2018). MEST itself is funded by Meltwater, a private sector company focused on social media analytics, media monitoring and competitive intelligence.

6.4 Key Actors

As a largely functional identity project, there is only partial collaboration with the public sector for certified identity as part of verification, though the exact nature of which officials in which departments, is not clear (Royal Academy of Engineering, 2020). The key technology partners are, of course, BACE-API as its own development arm.

6.5 Case Study Limitations

The full level association between the project and foundational identity associations are difficult to unpack (Bhandari et al., 2020). The case study is chiefly a private sector project, with *potential* public development *impacts*, rather than an actual public development programme. This limits the ability to draw direct conclusions on public development programming, though associations are noted.

7. Background

7.1 Digital Divide and Internet Penetration

According to RIA's demand-side data, Ghana has only 6% household Internet penetration, with broader penetration at 26% in 2017 (Gillwald & Mothobi, 2019). There is, however, significant mobile phone penetration (see Figure 1). The barriers to Internet use include the fact that 43% of the population do not know what the Internet is and that 14% are digitally illiterate (Gillwald & Mothobi, 2019). The CEO of BACE-API herself raised Internet penetration as a challenge for implementing technology solutions in Ghana (Fintech Circle, 2020).

COUNTRIES	MOBILE PHONE PENETRATION – AFTER ACCESS 2017	MOBILE PHONE PENETRATION – ITU STATISTICS 2016	INTERNET PENETRATION – AFTER ACCESS 2017	INTERNET PENETRATION – ITU STATISTICS 2016	AVERAGE SIM CARD PER SUBSCRIBER	MAXIMUM SIM CARDS PER SUBSCRIBER
Ghana	74%	139%	26%	35%	1.4	8
Kenya	87%	81%	26%	26%	1.2	4
Lesotho	79%	107%	32%	27%	1.3	5
Mozambique	40%	66%	10%	18%	1.3	3
Nigeria	64%	82%	30%	26%	1.6	5
Rwanda	48%	70%	8%	20%	1.5	3
Senegal	78%	99%	31%	26%	1.3	4
South Africa	84%	142%	50%	54%	1.2	5
Tanzania	59%	74%	14%	13%	1.5	5
Uganda	49%	58%	14%	22%	1.5	7

*Source: RIA After Access Survey, 2017; ITU Statistics, 2016**

Table 1: RIA After Access Survey: Regional Penetration Data, 2017

RIA's data demonstrated that 55% of Ghanaian household used mobile money services (second only to Kenya) (Gillwald & Mothobi, 2019b), with other reports stating there are around 14.5 million active mobile money accounts (Buruku, 2020). In terms of broader financial inclusion, 59% of Ghanaian have access to financial services (though Ghana has by some measures the fastest growing mobile money market). This facilitation of financial services through mobile has been acknowledged by Ghana's own

Digital Finance Policy, which has zero-rated all interoperable transactions made through the interbank switch (the interbank switch will be discussed in more detail later) (Buruku, 2020).

These digital divides have social impacts. There is apparently a low value for privacy concerns amongst Ghanaian citizens associated to collectivist attitudes (Dagbanja, 2016). And yet, particularly as privacy relates to personal data, some of this sentiment may also be associated with low levels of digital literacy. Digital literacy of course also a question of degrees; marginal users of the Internet may more passively consume online content, making them more susceptible to security and privacy risks (Gillwald & Mothobi, 2019).

In implementing their business plan, BACE-API noted how businesses – even in the banking sector – have low levels of "digital literacy"; but in fact, when a broader variety of interviews with the firm are considered, it may not be digital literacy, but rather low levels of digital *trust* which pervades both businesses and individuals (which might be associated with literacy, but can also be sourced from other social and cultural influences) (Fintech Circle, 2020).

7.2 Digital Economy and Regulation (of Financial Services)

Financial regulation

Ghana is one of the fastest growing economies in West Africa (Addai & Arthur, 2020). Within this growth environment, the use of digital banking has been specifically identified as central to Ghana's macroeconomic efforts (Buruku, 2020). Yet, financial asymmetry has been identified as a leading challenge in the financial services sector in Ghana, with Agyapong, (2020) noting:

> "...the issue is the availability, validity, reliability, and management of client information to inform credit-granting decisions".

There has been much proactive financial regulation in Ghana (other aspects of regulation in the environment are touched on later), but the broader environment may not be conducive to sound financial practice. This is why between 2016 and 2019 the banking regulator (the Bank of Ghana) took a series of hard actions in the sector, with eight finance houses having their operating licenses withdrawn, as well as 10 universal banks, 28 savings and loans companies, 347 micro-finance institutions, which had their licences revoked (Agyapong, 2020). The high number of licenses withdrawn from micro-finance institutions, in particular, is in sync with the increasing cynicism on the impact of the micro-credit boom experienced in East Africa in the last decade and a half (Izaguirre et al., 2018). The licences were, in fact, largely withdrawn because the institutions "…were found to be insolvent and did not meet the minimum capital legally required by the regulator…and some had excessive risk exposure" (Agyapong, 2020). In fact, one of the identified weaknesses of the microfinance institutions themselves are that they have "…inefficient and dated internal processes" (Agyapong, 2020). It is important to reflect on BACE-API's business model in terms of this context.

Mobile banking growth has started to outpace Internet banking. However, security fears and "cost issues inherent in its usage" still threaten broad acceptance of the practice (Addai & Arthur, 2020). The Bank of Ghana has launched a cashless project through the e-Zwich system (the details which are discussed in more detail under consideration of national biometric projects), however, it is not yet a viable alternative. A small quantitative survey taken of Ghanaian residents demonstrated that the actual usage of the e-Zwich was effected by limited access points and limited amounts of applications for e-Zwich transactions (Addai & Arthur, 2020). Additionally, social influence seems to be impacting use negatively, with one quantitative study indicating a statistically "…significant role [of] social influence…in the adoption of e-zwich" (Addai & Arthur, 2020).

Safety and security

Certainly, the existence of cybercrime is a notable challenge to fostering a good digital economy, with estimates projecting that Ghana lost $229.9 million to recorded cybercrime cases between 2016 and August 2018 (Allotey, 2018). The Head of the Cybercrime Unit of the Criminal Investigation Department (CID) of the Ghana Police Service, Chief Superintendent, Dr Herbert Gustave Yankson, reported that in 2017, $69.2 million was stolen from private companies through cybercrime, with a significant 40% of that portion being losses attributed directly to financial institutions (Allotey, 2018). While banks have been trying to respond by digitalising their processes and products, they are not keeping pace with the technological advancements of the criminals themselves (Agyapong, 2020; Baylon & Antwi-Boasiako, 2016).

Additionally, safety and security of personal and financial data implicate the cyber maturity of the state (Calandro & Berglund, 2019). Capability and maturity assessments are thus a precondition for exploring legal and policy interventions on the data and BDI environment (Razzano, Gillwald, et al., 2020). Back in 2018, a cyber maturity assessment of the country noted that while it was "steadily developing", there were concerns in relation to public awareness and cybercrime trends (Business News, 2018). Ghana has an established National Cybersecurity Centre, associated with the Ministry of Communications, which centres their cybersecurity strategies.[3]

7.3 National Biometric Identity

Ghana also has a specific identity context that must be considered. Many Ghanaians are undocumented (Central Bank, 2020). This form of invisibility to the state was a common colonial consequence, prevalent in systems that elected to ignore the vital registration of populations (Breckenridge, 2010). In 2001, the Ghanaian government announced the desire for a national biometric identity registration system, and the tender for such project was granted to Sagem in 2003 (in spite of large scale corruption being reported in relation to the company in Nigeria around the same time) (Breckenridge, 2010). Yet, working alongside the National Identification Agency (NIA), the project was inhibited by:

- the 'dishevelled' state of the Births and Deaths Registry, and
- difficulty in creating a 'workable test for citizenship' in a country with largely fluid borders and long histories of migration (Breckenridge, 2010).

In practice, citizenship decisions were largely made *ad hoc* by officials. Yet, in spite of the projects floundering, there was unanimous passage in 2006 of a law that enabled the compulsory gathering and storage of biometric identity (Breckenridge, 2010). And in spite of a period of significant growth and broad public support for the project, in 2008 the NIA began to run out of funds and – under a newly elected government – enthusiasm for the exercise waned, as did the provision of funding, leaving the most populous and most inaccessible areas of Ghana largely 'untouched' by registration activities (Breckenridge, 2010). In 2009, the dismissal of the Director of the NIA all but halted the exercise. These patterns almost entirely replicated the failures seen in the Nigerian biometric identification project (including the selection of the service provider), with financial and administrative failures eventually derailing it (Breckenridge, 2010).

Another public-sector driven biometric project, Ghana's E-Zwich project, became an interesting pivot in public sector biometric focuses. In 2008 the Ghanaian Central Bank launched an interbank switch (a

[3] Their website can be explored here: https://www.cybersecurity.gov.gh/.

networked, central database system that allows all banking transactions to be resolved), purchased and managed from South African company Net1 UEPS (Breckenridge, 2010).[4] The solution proposed by Net1 was designed for recruiting the 'unbanked':

> "The system developed by UEPS is, as [former CEO] Belamant has observed repeatedly, aimed at the very poor, illiterate people who 'are not going to remember the pin number on the card'. It is also specifically geared to the fact that networked communications infrastructure, and electricity, is generally absent in much of the African continent" (Breckenridge, 2010).

It was touted as the world's "first biometric money supply" as a move toward a cashless economy (Breckenridge, 2010). This was an effort for a more centralised role for the state in the regulation of the economy, which include the ambitions of bringing more citizens within formal banking, but also formalising a significant informal economy (see earlier discussion on Ghana's financialised development agenda) (Breckenridge, 2010). This move was a noticeable agenda shift:

> "e-Zwich [marked] a retreat from an older, and broader, project of identification that was designed to bring to the state's attention members of the poor, rural, young and old population who very largely had slipped out of sight in the twentieth century" (Breckenridge, 2010).

In other words, the more traditional development agenda of national and civil identity was replaced instead, heavily influenced by private sector and development partnerships, by digital identity largely for purposes of financialisaton and taxation. In the implementation of the system, there was a strong focus on criminality. The President of Ghana, when describing the project, was keenly attached to the notion of bringing the informal economy within the purview of taxation (Breckenridge, 2010). For the Central Bank, there seemed a strong desire to remedy the fact that the large majority of the population were still outside the formal banking sector (Breckenridge, 2010).

The cards could only be used through an e-Zwich machine and, outside of distributional challenges, interesting implementation challenges that emerged included:

- Difficulty in using and maintaining machines from the perspective of the merchants;
- Cardholders holding *shopkeepers* as responsible when there were insufficient funds;
- Difficulty in reading biometric fingerprints in the hardware;
- False positives in reading biometrics;
- Failures in authentication; and
- Most commonly: "Although the e-Zwich has been designed to support offline transactions between smartcards, merchant owners of the POS machines were required to complete a reconciliation with the central server at the end of every working day (or after 800 transactions). This connection was delivered though the wobbly cellular network, which meant that merchants had to have on hand, every day, a source of electricity, sufficient prepaid airtime to complete the connection and a reliable cellular single. Failures were commonplace" (Breckenridge, 2010).

The system creates a significant centralisation of data, wherein "…the e-Zwich records the biographical details, the times, places, and amounts of all transactions on the system." Importantly, research noted in 2010 that it is the 'success' of the e-Zwich that has been used as a rallying call for implementing other technological and biometric projects, such as biometric voting (Breckenridge,

[4] Net1 features in South Africa's biometric identity case study, as well.

2010). This, in spite of cautions in the literature of the challenges in implementation. Recent assessments of the e-Zwich project in particular have noted:

> "Transformation of the cashless sector remained at best in a confused state and at worst an awkward drawback. The devastating situation has forced users to snub the e-zwich smart card which has failed to bring relief and comfort in carrying out cashless transactions in the country and also to steer the country into a cashless financial society" (Addai & Arthur, 2020).

The recent foray into biometric voting in the national elections that were justified by e-Zwich, have in fact been the site of political contestation, with biometric systems themselves being raised by the opposition as sources of contestations against the final results. The Biometric Voter Management System was in fact resisted by a consolidated coalition, the Inter-Party Resistance against the New Voter Register (IPRAN) – although the coalition's activities seemed to have peaked prior to the general elections being held (Aikins, 2020). These kinds of political conflict on biometrics emerge within particular histories – the Electoral Commission has recently had a change in leadership, with emerging distrust over its institutional role feeding into cynicism for the inclusion of biometric registration solutions (Aikins, 2020). Yet the African Union, in its observer comments on the elections, cited the biometric registration process as a commendable success– noting "orderly and peaceful" elections (African Union, 2020).

In terms of the roll out of a national biometric ID, the Ministry of Finance noted that the NIA is currently once again engaged in implementation activities (Ghana Ministry of Finance, 2020). There are explicit plans for the national biometric ID to assist in e-KYC (Ghana Ministry of Finance, 2020). An impressive ethnography of the actors involved in the current national identification system has recently been provide by Thiel (Thiel, 2020), which highlights the challenges of diversification of both data types, data sources and data actors seeking to be coordinated in a centralised data vision.

Yet, as one researcher stated:

> "Visions of bright biometric futures continue to feed into political decisions and their communication to the general public" (Thiel, 2020).

This view doesn't consider though the political resistance to biometric identity programmes, and other data programmes, by both the official opposition party, National Democratic Congress and others (Aikins, 2020). The same researcher noted that the lack of civil society resistance to identity processing was notable in a time of intensifying contestations on citizenship and xenophobia in Ghana (Thiel, 2020). So, how might we reconcile these seemingly contrasting political perceptions? What is consistent in the political sphere is that biometrics and identity are a significant matter of the moment. In part, this may be because technological issues, given digital literacy and trust, can be met with cynicism and, are at the very least, easily politically manipulated as an issue. And certainly, narratives centring identity projects within the emerging discussions on the digital economy are important. Yet a considered history of the role of biometric and digital identity demonstrated how it has always stood as an important locus for social control.

7.4 Regulatory and Policy Environment

The broader economic, social, and political contexts of finance and identity also exist within specific regulatory conditions. Continuing from the discussions above on the financial services environment, the relevant regulatory history should be outlined.

Following an initial review of the banking environment, the governor of the Bank of Ghana (appointed in 2017), Ernest Addison, began continuing the reform of the banking sector that began from 2016,

which included the license withdrawals previously mentioned (Central Bank, 2020). This financial reform was supported strongly by the development communities, with the World Bank approving a $30 million International Development Association (IDA) credit in 2018 specifically to support Ghana in strengthening "…its financial sector stability and improve inclusiveness for users of formal financial services and the financially excluded, particularly women, rural communities and farmers" (World Bank, 2018). And the International Monetary Fund has identified the stronger banking sector as central to Ghana's strong macroeconomic outlook (Central Bank, 2020).

Interventions move beyond compliance regulation and extend to promotional activities. Plans are in place for a fintech regulatory sandbox for fostering financial service innovation (Central Bank, 2020). The implementation of the GhIPSS Instant Pay (GIP), which allows payments to be sent across financial institutions electronically from one bank account to another, is also contributing to fintech development, and the Central Bank will be launching a new FinTech and Innovation Office (Central Bank, 2020).

Political will includes the Ministry of Finance launching a Digital Financial Services Policy in 2020, in which supporting fintech is one of the six foundational pillars, with such support being envisioned as:

- Undertaking an assessment of the policy environment in place for fintech firms and investors;
- Assessing the need and feasibility of a regulatory sandbox for fintech products (a call already heeded by the regulator);
- Providing direct government support for fintech entrepreneurship; and
- Privileging fintech-based payment solutions for Government-to-Person and Government-to-Business payments (Ghana Ministry of Finance, 2020).

Importantly within the Digital Financial Services Policy, specific capacity-building on financial data issues with the Data Protection Commission is prioritised (Ghana Ministry of Finance, 2020). This form of inter-regulatory coordination, which particularly considers data governance, is cited as a central strategy for fostering a good digital economy (Razzano, Gillwald, et al., 2020).

This emerging prioritisation of fintech innovation has not yet fully reflected in the lived experience of firms that do that innovation. The CEO of BACE-API herself has stated:

> "[While] we are aware [government regulations don't exactly encourage innovation]…we have been working to build trust, educate our target, and build quality and secure products. Also, we signed strategic partnerships to get more support and drive our works. (Kolawole, 2020)"

Yet the broader tech ecosystem in Ghana is acknowledged by the CEO as being more conducive, generally:

> "When I moved to Ghana in 2017 [from Côte d'Ivoire], I saw a big difference; Accra had a more active tech ecosystem. I read about and met a lot of entrepreneurs who were doing great. Also, Ghana is an anglophone country, and we can't overlook how anglophone entrepreneurs have access to more opportunities, investment and can more easily [scale] their business in new markets" (Hastings-Spaine, 2021).

7.5 Legal

The broader legal framework of relevance to digital identity activities include Ghana's Data Protection Act, 2012. Within its preamble, the Act notes its objective is:

> "…to establish a Data Protection Commission, to protect the privacy of *the individual* and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters" [Emphasis added].

This individualised language within the data protection law has been of interest to researchers (Dagbanja, 2016), though it is fairly typical with international privacy frameworks. Article 18(2) of the Ghanaian Constitution provides citizens with a fundamental right to privacy. The Article provides that "no person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others." Importantly, unlike some African constitutions, a right to privacy of communications (considered the standard constitutional foundation for informational privacy) is included (Razzano, Gillwald, et al., 2020).

There is a Data Protection Commission in the country. The Commission understands the central contextual challenge it is meant to meet as being that:

> "…the barrage [of] privacy invasions of citizens in [Ghana] especially through the use of information technology, have led to discrimination, personal harassments, damage to professional reputations, financial losses and in some extreme cases death" (Dagbanja, 2016).

The incentive to pass the law was largely economic – with legislators seeking to satisfy the EU directive on cross-border flows, in spite of the social descriptions that are associated with the text (Dagbanja, 2016).

Ghana's legislative environment includes other laws of relevance, such as the Electronic Communications Act, 2008, which prohibits unlawful disclosure of certain user data. Similar sectoral protections (and prohibitions) are present in the Credit Reporting Act, 2007; Public Health Act, 2012; and Children's Act, 1998.

Additionally, there are laws of relevance to the national identity project such as the Citizenship Act, 2002, but that project is not the main site of this case study.

8 Analysis

8.1 Potential benefits

Biometrics will have an important role to play in combating fraud in financial services, but also in facilitating digitalised banking services in Ghana. African solutions for African problems, like BACE-API, can help to address the context of digital exclusion which not only threatens access, but also contributes to a distrust of technology solutions, by a fuller consideration on the inequalities at play. Consider for example the gendered dimensions of exclusion: in Ghana, 4 out of 5 women lack access to an account at a formal financial institution, compared to about 1 out of 4 men (Osabuohien & Karakara, 2018). If AI in BDI sought to be used to enhance inclusion, inclusion for whom? This is why the technological choices made are so important: the utilisation of facial recognition as a biometric, rather than fingerprints, by BACE-API is a noteworthy adaptation to the market, reducing hardware costs (Hastings-Spaine, 2021). It is also responsive to previous problems that were directly experienced by shopkeepers in trying to introduce the e-Zwich solutions.

BACE-API has sought to entrench itself as a fintech solution. This focus is no doubt encouraged by the Ghanaian government's own explicit support for the sector. Within this environment, notions on

"financial inclusion" and "banking the unbanked" are touted as the main social aims of the community. The association between identity and emerging forms of African capitalism as a particular economic nuance are immediately highlighted, a phenomenon that has been catchily termed as "Biometric Capitalism" (Breckenridge, 2020). Yet much of the hopes for "banking the unbanked" is the expectation the poor have cash that is not capitalised on due to financial exclusion; when the reality in our economic unequal contexts is that: '[t]he middle and upper classes control the country's wealth and they are generally [already] well-banked'" (Breckenridge, 2010). The development agenda does not necessarily match the business case, in spite of how the two narratives are spoken of jointly through out much literature. Nevertheless, mobile money is helping to bridge the financial access gap in Ghana, and thus there is certainly a market for products like BACE-API, which centre remote authentication through realistic technology choices.

There is though an incongruence to how BACE-API describes its own product versus its business model, which speaks significantly to the context of technology in Africa. Within their own pitch deck, for example, BACE-API cites that: "According to the World Bank's Development Identification Program (ID4D), more than 40% of people without an ID card in the world live in Africa. This contributes to financial exclusion and makes it difficult for businesses to identify their customers". The connections between financial inclusion, "banking the unbanked", and digital identity is a common trope within development agendas (Razzano, 2020b). And it is telling that so significant is this development narrative that it informs the sale of a product that is meant to be pursued through a B2B business model, which might better focus on business cost-saving and the potential for expanded markets. It is interesting to consider this in the broader AI ecosystem literature that is emerging: while seeking to position itself as a tool for "human flourishing" in the context of financial inclusion, the actual technological benefit being vested from the AI itself is efficiency and profit maximisation for finance service providers (Stahl, 2021). While efficiencies in financial services *may* improve financial inclusion, the potential benefit seems more remote – and dependent on a number of other structural influences – than may be being pitched.

8.2 Inequalities and exclusions

Digital inequalities intersect in a variety of ways within the AI4D context that provide a particular context for understanding what imminent risks and harms in the deployment of AI technologies are. Of course, digital inequalities can exclude the public (and consumers) from engaging in AI innovations, yet it is interesting to see too how certain inequalities influence the development of innovations themselves. The CEO of BACE-API noted, for instance, how the English language has inhibited the innovation sector in Cote D'Ivoire in comparison to the more amenable environment in Ghana. And digital inequalities can thus present challenges to companies in establishing their market not just to the public, but even within B2B models.

RIA's After Access survey showed that, though 71% of Africans surveyed did not have access to formal financial services, that figure rose to 81% of those in rural areas (Gillwald & Mothobi, 2019). And African residents who reside in urban areas (57%) are more likely to be financially included than those who live in rural areas (38%) (Gillwald & Mothobi, 2019). Of course, the costs of KYC compliance for businesses will depend on the specifics of the domestic regulatory context, but reducing these costs would be a sound economic benefit that remote verification could assist with.

Yet, there is not enough suggestion in the surrounding documentation that specific dimensions of inequalities that arose from the use of facial recognition technologies, such as gender bias (Buolamwini & Gebru, 2018), or cultural exclusions that may arise from facial markings, for instance,

will be accounted for within the design process. Functional identity projects will to be designed and implemented with these exclusions in mind: yet questions remain as to what positive obligations might be created on companies like BACE-API, to do this work.

At a broader level, exclusion in relation to national identity projects can often have gendered and aged dimensions (Center for Human Rights and Global Justice et al., 2021). With centralised digital identity projects of functional identity, exclusion from these systems also means exclusion from access to basic social protections and other services tied to those projects (Center for Human Rights and Global Justice et al., 2021). Gendered aspects to participation in identity project may result in specific challenges for women (Bailur, 2019). Additionally, while lack of access to identity in African communities had much of its source in colonial practice (Breckenridge, 2010), the use of biometric technologies and identities may yet again emerge as a mechanism of exclusion for "non-citizen" populations in the face of reinvigorated nationalist discourse globally and regionally (Thiel, 2020). It remains to be seen how conversations on facilitating population flows for the emergent digital economy, will balance against nationalist and even populist narratives on citizenship (with identity as the ultimate verification standard). And it is yet it is unclear at the national level too how these exclusion risks will be considered in national projects. Yet the obligations on public sector actors, given constitutional and administrative parameters, are often clearer than for private companies (Razzano, 2020c).

In other words, exclusions should form a central part of risk understandings. But the specificities and exclusions that arise directly from a private sector technology like BACE-API, in its infancy in terms of implementation, can only be speculated.

One particular dimension of note in the case study is that of gender within the innovation process itself: BACE-API is headed by a woman, in a technology environment still heavily dominated by men (according to Disrupt Africa, only 22% of start-ups have at least one female founder) (Salaudeen, 2020). Charlette N'Guessan is not just the CEO, but was also the first woman to win the Royal Academy of Engineering's Africa Prize for Engineering Innovation (Salaudeen, 2020). The youth of the company means it is difficult to assess how a female CEO might influence, the transition and practice of the company itself, but it is worth reflecting on the lived experience of the CEO herself:

> "I have a purely scientific background. I have evolved in an ecosystem dominated by men. I know the realities and challenges of this ecosystem. As a woman who has carved out a place for herself in this industry, I believe my experience can inspire other young women and girls to pursue careers in tech. I like to collaborate and support actions that aim to promote gender equality in the field of technology.
>
> In particular, I think we need to invest in educating women because at the end of the day what matters are skills, not gender. Society must break down barriers and stereotypes related to women in engineering, and we must create more opportunities" (Bajaj, 2020).

The CEOs downplaying of her own challenges as a woman in engineering are consistent in her interviews, where she has made statements such as "I feel lucky to work with men who understand that it's not about being a female" (Hastings-Spaine, 2021). In a way, she confirms the female success is an anomaly in technology – but is still also heavily reliant on the attitudes of the men in the immediate circle of an individual.

There can be no doubt that the ability of AI4D technologies to manage gender, and other, inequalities, will be influenced by the ability of innovation communities themselves to forward diverse capabilities (Sen, 2005). Yet the exclusion that AI facilitates has already begun to demonstrate gendered

proclivities in regions with more advanced AI projects (Buolamwini & Gebru, 2018). AI solutions will not be a magic salve to gendered (and other) exclusion, as evidence is already starting to demonstrate. Instead, the structural impediments that result in many of these exclusions (sometimes embedded in the technologies, sometimes the data, or even the business model, etc..) may be reproduced through the technologies themselves. Technologies like BACE-API should be monitored closely, particularly to see if the ability of African female-driven development can directly begin to start meeting at least some of the challenges that currently seem embedded in AI development.

8.3 Governance

The BACE-API leverages data to train AI in a manner that can better verify African faces. It is also able to verify identity through access to public sector data. While not much detail is available about the exact nature of the relationship between the business and the public sector, certainly what helps facilitate the relationship is that Ghana has an emerging data governance framework in place.

The Ghanaian government has focused significant policy energy on the financial sector, speaking strongly of the association between advancing fintech and the broader macroeconomic goals. This focus of their digital economy underscores the relevance of facilitating data flows, whilst ensuring privacy protections, as a central policy issue for African development (Razzano, Gillwald, et al., 2020). The data is the root of BACE-APIs business model, with the AI standing as the value-add.

Ghana is demonstrating a strong political will to put in place a regulatory framework that might foster financial innovation, in particular. The focus on cross-sectoral regulatory collaboration is a strong feature of the policy solutions posed; and while CEOs of companies like BACE-API may still cite regulatory challenges, business innovation is supported by policy innovation – solutions like regulatory sandboxes, inter-regulator capacity-building, and others are a necessary step for ensuring African-driven solutions. In contexts where AI innovation is largely nascent, immediate steps should be taken to encourage domestic innovation (that includes data within its remit). Strong regulators will be able to address the economic and social risks that accompany technology innovation, and already have begun to do so in countries like Ghana and South Africa (Breckenridge, 2020). But as with other African data protection environments, the ability of the institutions to be efficient regulators – as with Ghana's Data Protection Commission – depends significantly on implementation and sustained political will (Dagbanja, 2016; Greenleaf, 2011)

Yet, given sustainable development goals and the public aspect of many of the gains AI technologies might seek to address, will the role of the public sector merely be creating a 'conducive' environment, rather than instilling its own contributions directly to research and development? While the case study didn't begin to answer that question given its project focus, it is a research question that arises as fundamentally important from the broader themes.

8.4 Human rights

While privacy is a fundamental human right, the background context helps to ground how collective aspects of these rights will be profoundly important in shaping the AI development agenda (Razzano, 2021). The colonial project was largely one of exclusion of indigenous populations, and actively rendering indigenous needs as invisible (Breckenridge, 2020; Mhlambi, 2020). Biometric and identity projects must be understood in the context of populations who have been less visible to the state than they should be. This context is important, as often consideration of the lack of "privacy" norms in African contexts is attributed either to low levels of digital literacy, or to collectivist understandings of rights that have marred the passage of a "right to privacy" in regional instruments previously. Yet,

they may fail to consider the benefits to being visible that may form a significant part of an individual's privacy calculation (Razzano, 2021).

The value of protecting privacy goes beyond the protection of the dignity of the individual (Burchell, 2009; Naude & Papadopoulos, 2016). The notion of ubuntu (the African principle 'that we are human through others'), which informs much contemporary African human rights theory on collective rights, also helps demonstrate how it is the relational aspect of our personhood that normatively underpins its value (Mhlambi, 2020). Notions of ubuntu and collectivist protection do not exclude ideas of privacy, but rather adapt them(Mhlambi, 2020). Identity is a social programme, pursuing an important social end. Broader collectivist privacy understandings form an important balancing principle within the digital identity rights frameworks.

There are specific human rights dimensions of identity, as well, in relation to legal applicability as well as citizenship. Article 6 of the Universal Declaration on Human Rights stipulates that "Everyone has the right to recognition everywhere as a person before the law", and the association between access to identity as a mechanism for facilitating and enacting other rights has centralised it within development discourse. So, for instance, the SDGs set a target in 16.9: "to provide legal identity for all, including birth registration by the year 2030". The Constitution of Ghana's rights to citizenship are given effect through the Citizenship Act, 2000. However, the broader identity rights remain more relevant to foundational identity cases.

8.5 Risks and harms

Data breaches stand as a key risk in the biometric and digital identity space. Yet other risks associated to unsound data practices like mass collection and function creep remain central in foundational identity systems, in particular (Sandhu & Balakumaran, 2017).

The use of mobile technologies at the point of the user helps to mitigate some of the risks associated to constant electricity and Internet supply at least at the point of data entry (Privacy International, 2019), but of course these are direct challenges to trying to design and implement innovations.

Yet what a (chiefly) functional identity systems like the BACE-API case study helps to highlight is how the context of the function is important too. Another risk, particularly where financial 'inclusion' intersects with digital identity, is that the 'development' purpose of visibility for financial inclusion may not necessarily result in reducing inequality and poverty.(Izaguirre et al., 2018; Razzano, 2020b).

8.6 Identity Politics

The trajectory of the national identity project has lessons for the political economy of "Biometric Capitalism" in Africa. Political contestations have derailed the passage of the national identity project, and recent happenings in relation to the Ghanaian elections have well-demonstrated how identity and biometrics can be an interesting political football, which may impede or improve targeted identity interventions – but at its most basic, makes the implementing context challengingly variable. A component of the political challenge is of course the public-private nexus of these initiatives. In speaking on "Biometric Capitalism", Breckenridge noted rent-seeking could contribute to authoritarianism and corruption (Breckenridge, 2020). In Ghana and Nigeria, the same actors dominated biometric projects (and resulted in similar criticisms of corruption). Without delving into the monopolisation issues as a regulatory feature, African innovations will seek to compete in an environment in which exclusionary collaborations are rife, not least of all because of the costs involved. It is interesting to compare the long-term derailment of the national identity project with the

comparative implementation of the e-Zwich project. Though of course they are greater structural impediments to national and civil registration given their scope, and requiring different stakeholder collaborations, the financial imperatives that support the e-Zwich system (and potentially the BACE-API innovation) seem to at least have more consistent political support.

9 Key Case Study Findings

The BACE- API case study is an example of a private sector led, functional identity system that uses AI for facial recognition. Though the purpose of the technology is framed within development goals, the realities of the technology to combat financial exclusion – when it does not of course seek to deal with the structural impediment underpinning that exclusion – are questionable. Additionally, the challenges in opacity within private sector interventions make identifying specific harms associated to those AI technologies and seeking to mitigate risks, immensely challenging. African solutions to African problems will first have to deal with the challenges within the innovation environment, variability in the policy and regulatory environment, and then directly tackle the digital inequalities that mark that context. Exploring a strong business case on top of those preliminary hurdles then becomes the goal to grow from funding-dependent models.

- Even in Ghana where there is a particular appetite for fintech development, the political economy of identity presents challenges for embedding AI technologies in the intersections between these two fields.
- Whilst it is difficult to extract details on the form of the AI technologies (and importantly, the dynamics of the data underscoring them), that is in itself a finding: the proprietary nature of technological development in AI (and not just 'black box' technologies themselves) will continue to make it a challenge to monitor the social and political dimensions of these products.
- Sustainable development goals and AI for human well-being may be significant purposes for such technologies, but in practice it can already be seen how these "objectives" and "purposes" may be used to whitewash over the real imperatives underscoring technologies, which will continue to present challenges to AI implementation (Gurumurthy & Chami, 2019).
- Identity projects arise within a particular social and political history of exclusion for many African populations. This will need to influence what we consider useful interventions to be, but also means it will be a reality that a significant area of AI technology will relate to identity authentication processes in the near future (which means creating norms and standards for these kinds of activities should be a research priority).

Part D: Being Seen for Services in RSA AI

10 Introduction

In January 2021, footage of water hoses being turned on social grants recipients in South Africa became the indelible image of grants distribution during the COVID-19 crisis (Payne, 2021). Social grants form a central state development activity in South Africa: 45, 2% of South African Households *depend* on social grants (Statistics South Africa, 2018), and it remains one of South Africa's most effective poverty alleviation policies (Leibbrandt et al., 2015). And while the practice of social grants distribution and biometric and digital identity have been intrinsically linked for a significant period of time in South Africa (Breckenridge, 2014), exclusions from social protection systems have often directly been linked to challenges in both digital and non-digital identity.

Like other areas of technology, there are emergences with AI adaptions for efficiencies. And interestingly too, these intersections seem to be accelerated through the role of certain kinds of AI technologies within the context of the COVID-19 crisis (and social protection solutions).

Given that the majority party, the African National Congress, has recently formalised the intention for a Universal Basic Income Grant (Mahlaka, 2021), the social grants programme is only likely to expand. Exploring the intersections of AI and biometric identity in this context is clearly a prescient policy area. It is also a context in which public-private partnerships have an incredibly important impact, one that casts interesting shadows on newer iterations to integrate technologies (and AI) in public sector practice.

While there are not concerted AI projects linked to the national identity programme in South Africa yet, there is a product case study in AI that intersects with social development (and may in time have important implications for the practices around biometric identity). This case study therefore examines the use of GovChat, a cellphone application using AI-based natural language processing, being incorporated within social protection programmes, as the specific site for analysis.[5] Again, it is worth noting that this is not associated to any foundational national identity project, but is rather a demonstration of some of the key intersections in thematics on identity, social development and AI, we believe will have research relevance moving forward. Importantly too, it has been the subject of certain litigation that has helped to exemplify particular thematic intersections on both competition, and public-private partnerships.

11 Defining the Case Study

11.1 Technology

GovChat, is at its essence, a citizen engagement platform, which can be engaged through WhatsAPP and Facebook Messenger, and also through Unstructured Supplementary Service Data (USSD) (Plantinga et al., 2019). The 'future' plans for GovChat have included the possibility of integrating AI in the form of "Artificial Intelligence" responses, "Predictive Trends mapping", and "Natural Language query input" (Plantinga et al., 2019). However, as an immediate response to the COVID-19 crisis, a COVID-19 chatbot was launched through GovChat (developed supposedly in two weeks using Amazon Lex) to provide COVID-19 information and recommendations (Staff Writer, 2020). The current

[5] The public-facing materials on the application can be explored here: http://www.govchat.org/.

utilisations on AI therefore extend to natural language processing, with elements of big data analysis. Importantly, the machine learning potentiality of the product has been demonstrated in GovChat's latest iteration as a component of the South Africa's COVID-19 relief efforts: GovChat's machine learning-driven chatbot, "designed to improve the query-handling capacity within government and a number of other customers on a waitlist", was incorporated with the Department of Health's DOH COVID-19 Connect Platform to handle queries in relation to the Social Relief of Distress (SRD) grant (Malinga, 2020b) (impacts on the iteration will be discussed later and it will be referred to as the "SRD instance"). A GovChat chatbot was also used to engage with citizens through COVID-Connect to receive their test results, and assist in identifying contacts (Hunter, 2020).[6] Wherever possible, we will specify the precise instance being referred to.

GovChat is sometimes cited as having been introduced by the Cooperative Governance and Traditional Affairs Ministry, or as having "come out" of the Department, but the CEO has instead noted that GovChat has been "co-created" with the Department (and other Departments, as new iterations were developed) (ENCA, 2021). The actual tech development is driven by GovChat's partner, Synthesis Software Solutions (early development was done in partnership with the non-profit Praekeldt Foundation) (Farlam SC & Kelly, 2020). Synthesis Software Solutions fall under the portfolio of Capital Appreciation, who recently provided GovChat with funding (Mzekandaba, 2019).

Significant technological challenges arise from dependencies of GovChat on the WhatsApp platform for much of its services; this reliance is, in many ways, born of the fact that WhatsApp is South Africa's most widely used messaging platform, and thus reliance from a scaling perspective is seemingly unavoidable (Farlam SC & Kelly, 2020). This becomes a manifestation of the scale and network effects born of WhatsApp's significant user base.

11.2 Business Model

GovChat is registered as a private company, and was registered in 2016.[7] Ownership vests in the CEO, Eldrid Jordaan; the companies head of Finance, Tandi Aslam, but also in Michael Ivan (Motty) Sacks who's company – Capital Appreciation – provided a direct funding investment of R20 million (Mzekandaba, 2019). In 2019, the same three Directors also registered #LetsTalk as a private company.[8] The objective of the second registration was apparently to create a related company that directly served private sector companies (unlike GovChat, which chiefly seeks to serve government customers), though those separations became blurred significantly when the SRD instance of GovChat was instituted (and has been the subject of some concern from WhatsApp as the hosting platform) (Wilson SC & Berger, 2021).

The cost of product development so far is alleged at R 50 million (Wilson SC & Berger, 2021).

11.3 Stated Purposes

In describing their broader company mandate, GovChat state:

> "GovChat is South Africa's largest civic engagement platform accessible online, on any mobile handset and feature phones. We've enabled Government to speak to citizens directly at no

[6] The case study will largely focus however on linkages to the SRD grant information provision given the broader contextual factors that are examined as important.

[7] Registration details are available through the Companies and Intellectual Property Commission of South Africa.

[8] Ibid, using "Hashtag LetsTalk".

> cost, **while receiving service delivery related messaging in return**. GovChat exists through partnerships with the South African Local Government Association (SALGA), Department of Cooperative Governance and Traditional Affairs (COGTA) and Government Communication and Information System (GCIS)" [Emphasis added].[9]

Much of their social media and promotional material frame their central product as a civic engagement platform. Given the described AI components of its product though, they largely manifest within the efficiency stream such technologies offer – through utilising machine learning to improve communication efficiencies, in particular (Plantinga et al., 2019; Stahl, 2021).

11.4 Roll-out and implementation

Part of both the challenge, but also interest, in considering the Govchat platform is how many different iterations it has had (although the AI incorporation of interest was largely through the chatbot feature as it relates to the SRD instance). What is particularly noticeable in the implementation of the various instances, is that there are a variety of versions being launched very quickly in order to meet shifting needs of the different public sector partners. So, while the general purpose may be civic communication, functional purposes shift notably given the instance concerned.

We will consider some of the underscoring data collection and storage aspects of this under our later analysis.

11.5 Key Actors

GovChat has formal partnerships with several government departments, but has so far offered many of those collaborations for 'free' (*Question NW973 to the Minister of Social Development*, 2020). The company has formalised government partnerships with the Independent Electoral Commission and, importantly, the Department of Social Development, Department of Government Communication and Information System (amongst others), as well as with the United Nations Children's Fund for a domestic advocacy project (Malinga, 2020a). GovChat will have a B2B business offering through #LetsTalk, although distinctions between the two separate businesses are already muddied (Wilson SC & Berger, 2021).

GovChat itself is provided with technological capacity support by Synthesis Solutions, which seems to have been a direct result of Capital Appreciation's funding support (Mzekandaba, 2019). Previously, this support was provided by Praekeldt who – rather than being a private company – have two arms: a foundation, and a public benefit corporation status (Farlam SC & Kelly, 2020).

11.6 Case Study Limitations

Similar to the Ghana case study, the intersections with any foundational digital identity project have not been established. As an interview with a product owner in the field of biometric and digital identity in Africa noted in interviews,[10] the separation from foundational projects for many private sector and social entrepreneurship initiatives is intentional: foundational systems in Africa can be unreliable, and partnerships with the state at that level challenging to maintain consistently to ensure product quality.

[9] Their organizational profile (inclusive of blurb) can be viewed at: http://www.govchat.org/

[10] The interview was conducted 30 April 2021, though the respondent wished to remain anonymous.

The annual financial reports through the Companies and Intellectual Property Commission user portal were not yet available, and so secondary sources were relied upon for establishing financial details and business models.

12 Background

12.1 Roll-out Challenges

As more specific contextual background to the case study itself (and for subsequent analysis), it is worth outlining particular litigation of relevance. In 2021 South Africa's Competition Tribunal issued an interdict against Facebook to prevent it offboarding Govchat from WhatsApp (McLeod, 2021). The nub of WhatsApp's offboarding was that GovChat, by representing multiple different government departments as a proxy through one Business Account, was violating its terms of use. GovChat brought the interdict citing the significant public harm that could be instituted if GovChat services were to be disrupted, but sought this relief in the Competition Tribunal under the auspices of the threatened offboarding being an abuse of WhatsApp's dominance and motivated by anti-competitive motivations to engage in direct business with the various government departments themselves (Farlam SC & Kelly, 2020). As an interdict, only prima facie of the required dominance and harm needed to be established, but the interdict did note that GovChat could also not "…onboard any new clients or users to the WhatsApp Business account. Also, they may not launch, expand or sell any new 'use cases' to these clients" (McLeod, 2021). The papers presented to the Tribunal outlined a convoluted story of the struggles in iterations, and divergent motivations between local clients and global platform business. In addition, they provide a valuable data source for unpacking the realities of the business models, data practices, and competing interests that are central to many technology applications that transverse the public and private sector (aspects of the litigation will be reflected on throughout the analysis).

12.2 Digital and social inequality

South Africa suffers from significant social and income inequality, with its Gini coefficient measured at a startling 0.63 in 2015. One of the most significant drivers of this inequality is labour market incomes (Leibbrandt et al., 2015). A consequence of this inequality is the need for a significant social protection network. The South African Social Security Agency (SASSA) oversees and administers South Africa's social grants system. South Africa has a profoundly influential social grants project, which forms part of a strongly socially-focused expenditure – for the 2021-2022 period, of the R 2.02 trillion budget, R 335.3 billion was assigned to social development.[11] Social support is also keeping people alive. Statistics South Africa released the results of its General Household Survey in 2018 indicating that 45.2% of households interviewed depend on social grants, which renders over 17 million people reliant on these grants from the state (Statistics South Africa, 2018).[12] Currently, the social grants are distributed by SASSA through the South African Post Office (SAPO).

Significant job losses and contracted income opportunities as a result of the COVID-19 pandemic necessitated the specific SRD grant as a form of additional relief for citizens (Jain et al., 2020). The SRD grant only went directly to about 20% of workers who were actively employed in February but not employed by October, but 40% of these that *had* lost work were part of a household, which received at

[11] Vulekamali, *South African Government Budgets* [website], 2019, https://vulekamali.gov.za/, (accessed 03 January 2020)
[12] Statistics South Africa (2018) *General Household Survey,* available at: http://www.statssa.gov.za/?s=general+household+survey&sitem=publicatio

least one SRD grant (Bassier et al., 2021, p. 3). Yet research showed that "…South Africa's established pre-covid grant system remains crucial and accounts for the majority of those covered by social protection" (Bassier et al., 2021).

South Africa's inequality also has digital dimensions, though it has comparatively high Internet penetration in contrast to many countries in the region at over 50% Internet penetration and 84% mobile phone penetration (although with only 11% household penetration) (Gillwald & Mothobi, 2019).There are also significant dimensions of inequality in access across gender, location and education lines (Gillwald & Mothobi, 2019).

This digital inequality was not without direct impact during the COVID-19 crisis. When reflecting on the implementation of COVIDConnect (the instance of GovChat related to the sharing of COVID-related information), while part of the challenge lay in its ability to locate 'weak links' and also individual difficulties in establishing (or even remembering) previous contacts, part of the challenge was that between 30% and 40% of people in South Africa don't use WhatsApp at all, and while the 'user journey' on the portal costs less than 2 cents, this still would clearly inhibit efficacy if there is no data or airtime on a phone (Nortier, 2020). Low tech solutions are required to meet the needs of citizens – the low prevalence of AI in solutions may be conditional, but it is also a design response to the context.

12.3 Social protection and biometric identity

Some background to challenges in grants distribution in South Africa helps contextualise core challenges in intersections between digital identity and social protection, more broadly. In early 2000, a private company, Cash Paymaster Services (CPS), had been procured by the South African Social Security Agency (SASSA) to distribute social grants to citizens (Razzano, 2020c). Yet this arrangement had been marred by controversy, mismanagement and conflict - not least of all because CPS's other subsidiaries were said to be abusing the personal data of social grants beneficiaries to sell them over-priced products and policies, increasing grant beneficiary indebtedness to Net1's stable of companies (Net1 being the holding company for CPS) (Margele & Ngubane, 2018).

The privatisation of social grants distribution was authorised in terms of the Social Assistance Act 2004, 4(2)(a), but followed a 'modernising vision' of grants distribution in South Africa from as early as 1996, which would focus on interoperable databases and digitalised processes (Vally, 2016). There was always a perception that this digitalisation would require private sector assistance. And the desire for digitalisation was matched by an early desire by SASSA to institute a massive biometric data collection project as part of its functions. It is this biometric data collection, and processing, that in fact justified their original decision to tender CPS in particular, and once the contract was in place, SASSA began swiftly devolving the actual function of biometric data collection to CPS, viewing it otherwise as "duplication" (Vally, 2016).

Technological functions are often implemented through public-private partnerships in South Africa, in various forms. The latest strategic document from the Commission of the Fourth Industrial Revolution notes, for example, specifically on AI, that the establishment of an AI Institute should be established as a private-public partnership for supporting AI capacity-building (Commission on the Fourth Industrial Revolution, 2020). These functionary imaginings of development as delivered by the public and private will only grow with digitalisation, and then with Fourth Industrial Revolution technologies – a relationship of real import in the delivery of public goods (Gillwald, 2020; Ostrom & Ostrom, 1977).

The tender underscoring the CPS-SASSA relationship was declared invalid by the Constitutional Court following litigation initiated by a disgruntled tenderer. Yet, CPS continued administering grants in the interim as SASSA sought to try internalising the function. However, in 2016, a case was heard before the Constitutional Court initiated by a non-governmental organisation working with grants beneficiaries, which sought to try and ensure the distribution of social grants to South African beneficiaries was not disrupted as – in spite of the tender coming to an end - SASSA had not capacitated itself to take over the function centrally (through the support of SAPO).

While the crisis was averted through strategic litigation, the grants biometric identity demonstrates a kind of decentralised digital identity project specifically related to function, also referred to in the literature as a "functional identity system", but on a massive scale (Bhandari et al., 2020). Yet the national Home Affairs National Identity System (HANIS) (the foundational systems is discussed in more detail later), which stores national biometric identity, was always envisioned as having social protection authentication function too, which is expansive in comparison to national identity programmes in other countries (Breckenridge, 2005).

Something that was well-demonstrated in the CPS-SASSA case was that there were insufficient systems, either legal or practical, put in place at the time to safeguard beneficiary data between the two parties who both bore responsibilities for preventing misuse given how central biometric (and other) identity data was to the project. The delivery of social obligations through private mechanisms should not reduce accountability for that delivery. Whether sufficient lessons have been learned from that incident remains to be seen. In response to parliamentary questions directed at the DSD related to data protection measures in place in the GovChat partnership, DSD noted:

> "SASSA will have access and the full rights to the data will remain vested in the Data Subject as per the Protection of Personal Information Act. SASSA and GovChat have signed a Data Processing and Confidentiality Agreement which protects beneficiary data against access by any other party or sale of the beneficiary data or use for any other purpose other than for application for the special Covid 19 SRD grant….
>
> Upon termination of the payment of the Covid-19 social relief grant of R350, the collected data will be stored or disposed of in terms of the applicable personal data protection laws" (*Question NW973 to the Minister of Social Development*, 2020).

Specific concessions to the protections provided by the Protection of Personal Information Act (POPIA), 2013 (to be fully effective by June 2021 and discussed more below) are already indicating the shifting statutory parameters for engaging in personal data-centred activities.

Yet the centrality of digital identity and public sector collection of biometric data has been a practice that has long preceded the seemingly necessary data protection provisions to help manage it: in South Africa, the DSD has been engaged in biometric data collection to facilitate social grants distribution for well over two decades (Vally, 2016). This is not wholly out of keeping with other jurisdictions, such as India, which have also noted that:

> "As people who have been 'watched by default', low-income populations in particular may be attuned to trading theory details for welfare benefits" (Srinivasan & Oreglia, 2020).

Yet the modern association of the exchange of digital identity for social benefits belies an African historical legacy of vulnerable groups in fact being invisible to the state: one of the most significant barriers to accessing grants historically has been a lack of identity documents; for many citizens you

are not a 'person' to the state unless you are a 'number' too (Donovan, 2015). These dynamics are an important part of understanding the role of biometric identity in the South African state.

12.4 National digital and biometric identity

National identity is represented through a green bar-coded paper document, though a phased roll-out process has started to replace all such documents with a Smart Identity Card (Smart ID) (Government of South Africa, n.d.). The Smart ID card has on its face a person's name, identity number, citizenship status, sex, and country of birth. The ID card also securely stores biometric information (face and fingerprint currently) and has space to store additional secure information like voter information. Currently, you are not obliged to hold a Smart ID Card, but all newly issued identity documents are in the form of the Smart ID. However, Smart ID cards can only be issued from offices that have the "live capture system" (Western Cape Government, 2021). Additionally, they can be obtained by certain banks that use the system in-house (providing a very literal example of the associations between digital identity and financial services) (MyBroadband, 2020).

The national identity project in South Africa comes with complications, many of which have been articulated as part of the Department of Home Affairs (DHA) recent Draft Official Identity Management Policy (2020). Below is an overview of the data sources for the current National Population Register (NPR):

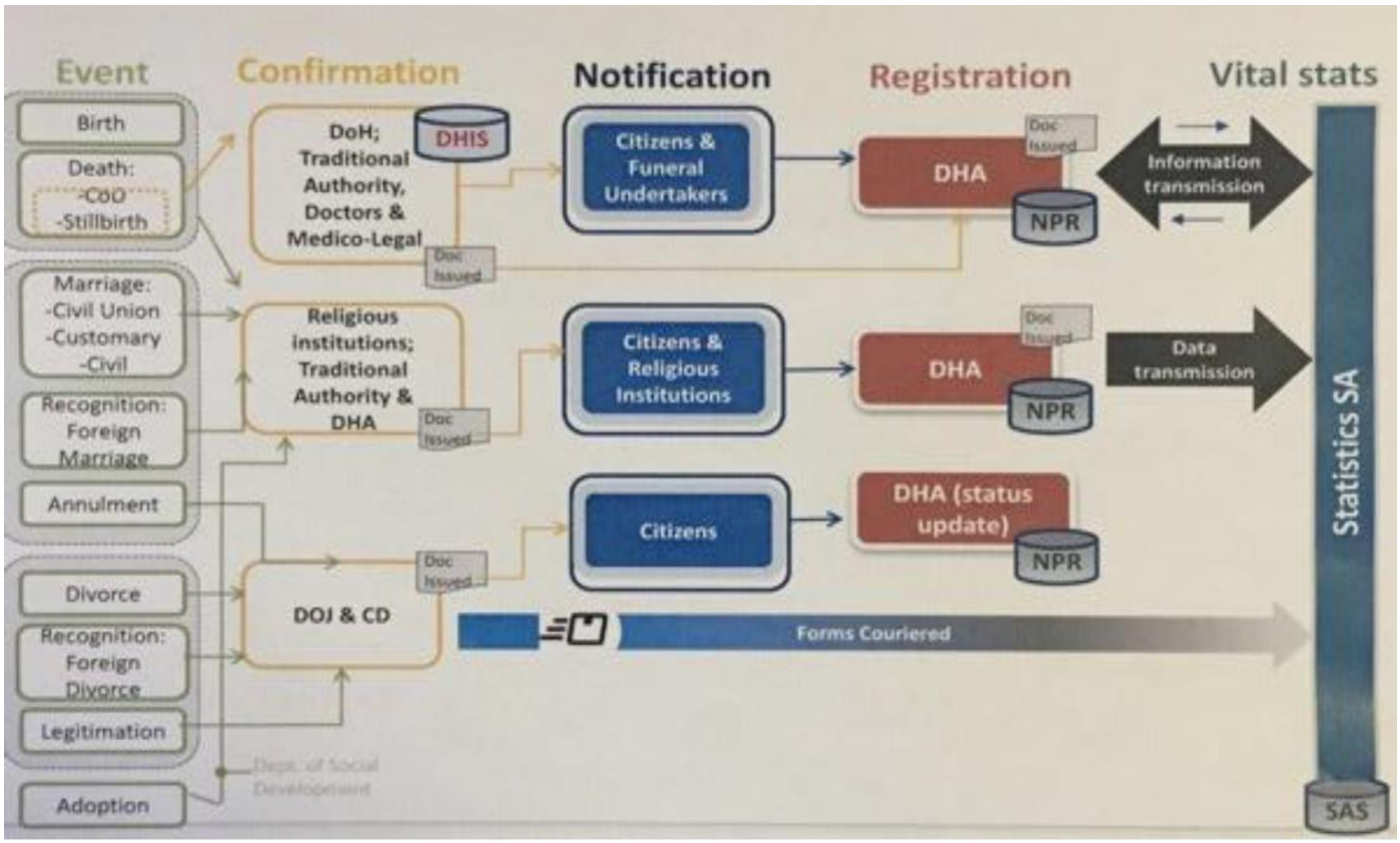


Diagram 3: An overview of the data sources for the National Population Registration (Department of Home Affairs, 2020b)**.**

Though national identity is the remit of the Department of Home Affairs (DHA), it is interesting to note from the above the decentralisation that seemingly has to occur in relation to identity confirmation (Department of Home Affairs, 2020a). Much of this has arisen from the need to centralise a variety of different identity sources as part of South Africa's national identity project after independence: this

project had to try and incorporate divergent administration systems of identity that resulted from segregationist policies, alongside both colonial and Apartheid preoccupations with biometric regimes for biometric control (Breckenridge, 2005).

Yet challengingly, these divergent sources are not interoperable across different systems. For example, the DHA notes:

> "…an update of the common data is not automatically updated on all the relevant systems that have the same data. This means that it is possible to change a person's ID number on the [National Population Register] without also changing the ID number on [Movement Control System] (and/or [Enhanced Movement Control System]). This effectively breaks the link between a person's data on the [National Population Register] and their data on the [Movement Control System] (and/or [Enhanced Movement Control System]), giving the appearance that the person has never travelled and rendering the person's data inaccurate" (Department of Home Affairs, 2020b).

As a response to challenges in national identity management, the DHA is seeking to establish a National Identity System (NIS) to replace the NPR. The proposed purpose of this exercise is improving national identity management for social benefit, but this new regime will emerge within a paradigm that now directly acknowledges lawful data processing:

> "According to international best practice, there are potential benefits of information sharing such as better government service delivery, improved risk management and cost savings as duplication of effort is eliminated. However, information sharing between state institutions, if not well regulated, can enable circumvention of individual privacy and data protection safety measures. The [POPIA] Act effectively grants the right to privacy as contained in the Bill of Rights and is widely regarded as being a codification of the common law position regarding processing personal data" (Department of Home Affairs, 2020b).

Yet grand "panopticon" style centralisation of national identity ambitions like the DHA's Home Affairs National Identity System (HANIS)[13] emerged outside of an existing data governance protection framework; the tendency of the state to collect data now and ask questions later is the data reality in which the emerging POPIA regime will need to try and manage (Breckenridge, 2005). The NPR was enabled to store biometric data as far back as 1982 (Breckenridge, 2005).

Perhaps unsurprisingly, a chief failing of concern in relation to the current NPR is the manner that it can contribute to exclusion. The current system of registration focuses on registration from birth, but associated to the status of parents, unintentionally resulting in:

> "…vulnerable groups [facing] significant economic and social barriers as a result. This group includes people who did not acquire birth certificates at birth, children of non-citizens who were born in South Africa, those who are excluded or improperly documented for historical reasons such as the borderline communities and Khoisan people, and abandoned children [and non-binary persons]. The new system proposes that every birth in the country, irrespective of the status of the parents, must be registered. At birth, the biometrics of a

[13] The NPR, which is used to record, store, and process citizens and permanent residents' biographic data, and limited biographic data for refugees. HANIS is used to store and process the biometric data of citizens and non-citizens (refugees, asylum seekers, illegal foreign nationals and permanent residents). This system will be replaced in the immediate future by the Automated Biometric Identification System (Abis), which will process and store biometric data of all persons, citizens and noncitizens.

> parent must be linked to the birth certificate of a child" (Department of Home Affairs, 2020b; Singh, 2021).

Children will then be required to be re-registered within the system at the age of 5 with their biometrics in the form of fingerprints and iris and facial photographs.

A further motivation for the revision of the system (again) is the need for sound digital identity management to facilitate trade, business and digital economy components of the 'Fourth Industrial Revolution' (Department of Home Affairs, 2020b). Yet these ambitions for digital efficiencies exist within a reality of logistical failings through its own existing digital infrastructure. As the Portfolio Committee on Home Affairs itself noted:

> "…the glaring and perpetual long queues that are evident at service points indicate the far-reaching implications of the impact of the lack of improvement within the IT environment" (Staff Writer, 2021).

12.5 Legal[14]

The broader legal framework within South Africa of relevance to digital identity activities include POPIA. Although the Act was passed in 2013, and various parts came into effect previously, including the establishment of the Information Regulator, the Act was in fact only fully in effect by 1 July 2020. Entities were again given a 12-month grace period in which to comply with its obligations. POPIA centres its provisions in relation to three key stakeholders (which does not exclude the public sector, though *some* public activities are exempt from *some* processing provisions):

- a *data subject* is the person that personal information relates to or identifies;
- a *responsible party* is the party that decides to process personal information in a certain way; and
- an *operator* is the person that processes personal information for somebody else. This person does not determine the purpose and the means for processing.

It provides a broad definition of personal information, considering it to be in essence information that identifies a living person. Processing covers all the different ways that someone's personal information can be handled by a responsible party or operator. It includes opening a file, reading a document, or even deleting or editing documents.

POPIA centres itself more explicitly across eight conditions that responsible parties need to comply with for their processing to be lawful. The conditions are (in cursory form):[15]

- **Accountability**: This means that the responsible party must take the lead in ensuring compliance with POPIA.
- **Processing limitation**: The responsible party must have a good reason for processing someone's information and try as far as reasonably possible to collect the personal information directly from the data subject.

[14] Much of this section is based on work done on a South African case study in partnership with the Association of Progressive Communications under the project title "African Declaration on Internet Rights and Freedoms (AFDEC): Fostering A Rights-Based Approach to Data Protection in Africa", which has as yet to be published. Once published, referencing will be amended of any further drafts of this research.

[15] Protection of Personal Information Act, 2013, sections 18-25.

- **Purpose specification**: The data subject must know about the purpose for which the responsible party is processing the personal information.
- **Further processing limitation**: The responsible party must ensure that if they will process that personal information again, it must be for the original purpose that they informed the data subject about.
- **Information quality**: The responsible party must ensure that the personal Information they process is accurate and complete.
- **Openness**: The responsible party must be open towards data subjects about how they process personal information
- **Security safeguards**: The responsible party and operator must provide appropriate and reasonable security measures against any risks that the personal information is exposed to.
- **Data subject participation**: The responsible party must communicate with the data subject about the processing and give the data subject to correct or update the personal information the responsible party is processing.

Transfer is a form of processing. Personal information can only be transferred out of South Africa if the responsible party ensures certain conditions are met. The main one of these conditions is that the responsible party has the consent of the data subject to the transfer. POPIA only allows for the transfer of personal information outside of South Africa to a country with substantially similar levels of data protection as POPIA.

Importantly, the law creates the Office of the Information Regulator (IRSA) to oversee compliance and act as an avenue for recourse, whilst facilitating regulation. The IRSA has been in place since December 2017, though quite resource constrained.

POPIA impacts a variety of laws, but is also being enacted within a particular legislative environment. Importantly, access to information is governed by the Promotion of Access to Information Act, 2000. PAIA creates a process for the request of information from both public entities, as well as private entities when required for the exercise or protection of any other right. POPIA has reallocated oversight and enforcement of PAIA from the South African Human Rights Commission (SAHRC) to the IRSA. This 'handing over' of powers has, however, not yet occurred – and has been delayed as part of the broader deferral of legal effectiveness POPIA (Razzano, Spuy, et al., 2020). To a degree, there are components of data and information protection within PAIA itself. While there is a right to request access to information, PAIA provides a mandatory grounds of refusal against a request of information if it would involve 'the unreasonable disclosure of personal information of a third party'.[16] Yet (and while POPIA has amended slightly the definition of personal information) the sections provided certain caveats to the refusal ground, for instance, not including information if consent has been given, or if it is in the public domain. There has also been a tendency in PAIA case law to interpret these refusal grounds quite restrictively.

There are sectoral laws which deal with personal data (as a subsect of identity management). The National Health Act, 2003 is an example of specific, statutory data protection for a sectoral information type. Another sectoral example of information protection relates to confidentially of information related to HIV-status, which is provided for children in the Children's Act, 2005. The

[16] Promotion of Access to Information Act, sections 34 and 64.

Health Professionals Council of South Africa has issued guidelines to similar effect, though this would obviously be qualified as per the National Health Act, 2003 which provides a public health exclusion.

The Electronic Transactions and Communications Act, 2002 was one of the earliest legislative interventions to try and engage on data protection, although chiefly within an e-commerce context (the early rumblings of digital economic activities in the country). The Act is largely recognised as a failure given its inadequate implementation. The National Integrated ICT Policy White paper, 2016 proposed a swathe of amendments to the law, many of which are in the process of being legislated (Gillwald et al., 2018).

In relation to the institutional aspects of identity management in South Africa, the Identification Act, 1997 governs the NPR and subsequent issuing of identity documentation. This is additionally impacted by the Alteration of Sex Description and Sex Status Act 49, 2003, which provides the process for people to have their sex alerted on the NPR and thus also have their identification documentation amended. A particular challenge in the South African landscape has been the amount of personally identifying information included with the actual *identity number itself*, which as per s 7 is compiled to include particulars of a person's date of birth and gender, and their status as a South African citizen. The NPR itself then of course compiles a significant amount of biographical data of each entrant, though it is not broadly publicly accessible, which includes as per s 8:

1. his or her identity;
2. his or her surname, full forenames, gender, date of birth and the place or country where he or she was born;
3. if he or she has attained the age of 16 years, his or her ordinary place of residence and his or her postal address;
4. if he or she is a South African citizen but is not a citizen by birth or descent, the date of his or her naturalisation or registration as such a citizen, and, if he or she is an alien and was not born in the Republic, the date of his or her entry into the Republic, and the country of which he or she is a citizen;
5. the particulars of his or her marriage contained in the relevant marriage register or other documents relating to the contracting of his or her marriage, and such other particulars concerning his or her marital status as may be furnished to the Director-General;
6. a recent photograph of himself or herself, if he or she has attained the age of 16 years;
7. his or her fingerprints, if he or she has attained the age of 16 years;
8. particulars concerning passports and travel documents granted to him or her;
9. after his or her death, the required particulars furnished when notice of his or her death was given, and on permanent departure from the Republic, the date of such departure, and particulars concerning the cancellation in the prescribed manner of his or her identity card or that card with the exception of the prescribed section thereof (if any); and
10. any other particulars determined by the Minister by notice in the *Gazette* as particulars which, subject to the conditions, exceptions or exemptions (if any) mentioned in the notice, shall be included in the register.

As can be seen, biometric data is already included, though the forms of biometric data can be simply expanded upon through regulation and notice.

13 Analysis

13.1 Potential Benefits

If the goal for exploring AI technologies can become about inclusion and the achievement of human flourishing (Stahl, 2021), the efficient delivery of basic services becomes an important public sector AI development agenda. When the delivery of social grants was returned to the public sector in partnership with SAPO, beneficiaries were compelled to change their cards (for receiving their payments) and 65% of those beneficiaries had to wait in queues of 30 minutes or longer (this of course does not include travel time, etc.) (Black Sash, 2018). In considering the SRD relief grant, facilitating applications through a digital channel only takes one so far (recalling that 30-40% of South Africans do not use WhatsApp) (Nortier, 2020). Yet, limitations in physical access to grant distribution points do highlight the fundamental urgency of growing the channels to access services – digital technologies may assist the public sector in leapfrogging some of the infrastructural challenges in logistics that have arisen in relation to social development delivery (Breckenridge, 2019), but perhaps ironically is unable to do that effectively without overcoming the existing ICT infrastructural shortcomings (Gillwald et al., 2018). Yet in all of this, the actual ability of AI itself to provide direct benefits is not being demonstrated in practice – in no small part due to the exceptionally nascent stage AI development is at in South Africa as a public service tool.

Facilitating sufficient and effective access to grants will impact millions of South African lives. Given the cited gains from incorporating AI, but also simply embedding technological solutions within previously paper-based services, it is however useful to reflect on the realities of using the SRD application. Annexure B contains separated screenshots of the applications interface and a user journey of trying to use it.[17] Of note was the inability of the service to recognise the “FAQ” instruction multiple times, regardless of how it was inputted. It is interesting for an application in which AI’s support of natural language processing has been so widely touted as a product value-add, that a very simple instruction – exactly inputted to instruction – cannot be ‘understood’. It is notable that this error re-occurred over two separate days when the application was tested.

There are additionally some challenges in the user interface, which make it a challenge for users (though they do not implicate the AI function). For instance, as can be seen in Annexure C the “Cancel” function does not, as stated in the instructions, act as a ‘back’ button. There are other implications for this though – although the product is touted as a civic engagement tool, it is really a civic communication tool as there are limited feedback loops (for instance, a receipt of an SRD could be considered a feedback loop of course, but much of the interaction is mechanical). This does not diminish the products value – a productive use of AI to facilitate effective service delivery communication could be of dramatic utility; but the realities of engaging with the product somewhat undermine the use statistics that have been used to evince its efficacy.

Further, as mentioned under the purpose, the efficiencies provided by the technology can lead to very direct cost benefits in terms of service delivery: the company itself claimed that in the first month of use of the SRD instance, the platform handled 413 032 individual queries, amounting to an average of over 13 500 individual queries handled daily (comparatively the company submit individual call centre agents can offer assistance to about 50 individual queries a day) (Malinga, 2020b). And apparently since the inception of the SRD instance, four million applications have been made through the platform (Falken, 2021). Across instances, the platform facilitates between 400 000-600 000 messages

[17] The screenshots are available as a single, rolling screenshot, but were separated out to make them digestible to read.

between users and government a day (Farlam SC & Kelly, 2020). That kind of volume would make a natural partner to machine learning applications.

13.2 Inequalities and Exclusions

GovChat demonstrates functional digital identity. Yet, as ambitions in the South African public sector grow for a grand plan "panopticon" of centralised, multi-function national identity (Breckenridge, 2005), it has to be noted that the foundations are already exclusionary. South African Smart ID cards are only available at some DHA offices (although mobile units are being rolled out – unsurprisingly as a response to the announcement of the local government elections) (*Question to the Minister of Home Affairs - NW1176 | PMG*, 2020). Or how the NPR itself already excludes many:

> "Poor people, rural residents and many elderly people face logistical and travel challenges. The direct and indirect costs such as fees, travel and lost wages associated with the application for, or use of, identity credentials are prohibitive to them. They also lack smartphones or other resources to access online or digital services or use credentials. The elderly also have difficulty providing biometrics and have limited access, or literacy to access, digital services. Persons with disabilities also lack mobility and/or accessible centres, which may hinder registration. The DHA may also lack trained staff and accommodating enrolment procedures. People with lower levels of literacy have difficultly completing applications as forms are either written in English or Afrikaans" (Department of Home Affairs, 2020b).

The early stages of digitising identification are already demonstrating an ability to exclude many South Africans, not least of all because of unequal Internet access and digital penetration (Gillwald & Mothobi, 2019). Thus, as has been seen in other countries (Center for Human Rights and Global Justice et al., 2021), the expansion of social protections functions to centralised foundational identity will only replicate the existing exclusions that degrade those systems.

Reflecting more directly on the SRD grant system, grant distribution has always been marred in challenges of exclusions of those that should benefit, and inclusions of those that shouldn't. Yet the Govchat solution will only be a salve to some applicants, and not all, given digital inequalities that may mean limited access to data and WhatsApp, although a USSD service was provided. Yet it is important to consider how the user challenges highlighted in the 'Potential Benefits' can be a direct form of exclusion, implicating improving the user-centred design processes around the product.

13.3 Governance

Global governance

The emergence of domestic AI solutions like the SRD instance can nevertheless mean reliance on global, oligopolistic systems and platforms, like WhatsApp (owned by Facebook). It is highly likely that AI will begin to expand these dependencies, as the relationship of data to AI is functional and central: training or machine learning aspects of AI rely on big data (as it does to several other general-purpose technologies, but that data is controlled efficiently by a few dominance firms (who often access and control that data through owned platforms like Facebook and WhatsApp) (Casado & Lauten, 2019). And this insatiable appetite will mean a particular value for data - already starting to emerge as a market force through realities like data-as-a-service (Morozov, 2018). This is a notable trend, because it speaks to growing drives for trying to manufacture excludability. Excludability is a method for asserting ownership of a private good (Ostrom & Ostrom, 1977), yet realistically the nature of data – which can be replicated and held by multiple people at the same time without impacting each other's

use – means that using laws to manufacture ownership (chiefly forms of Intellectual Property and Copyright law) can be challenging in spite of these incentives.

In addition though, in the context of public sector demands for AI, the network effects of global products like WhatsApp seem incredibly important for the delivery of broad services (like communications, in the case of WhatsApp); yet as WhatsApp's noted in its Heads of Argument, can the network effects of its broad consumer base really be the basis for a challenge in competition (Wilson SC & Berger, 2021)? Put another way, how can local innovation companies compete even in domestic markets when global players dominate so significantly (Couldry & Mejias, 2018)? And when these two seemingly conflicting incentives arise, the ability of domestic tribunals - like South Africa's Competition Commission – to provide effective relief in preserving local interests will be difficult.

Public-private partnerships

Certainly, consideration of the case study has reiterated how the interplay between the public and private sector is a key nexus for exploring power dynamics that arise from attempts to implement both digital technology, and later AI, in a development context (Razzano, 2020c, 2020d). Presciently, the CEO of GovChat Eldrid Jordaan himself noted:

> "Through the technology that we have co-created, GovChat and the South African government are demonstrating the possible future model for public-private partnerships," (Mzekandaba, 2020).

The co-creation of technology products that GovChat speaks to frequently (Farlam SC & Kelly, 2020; Mzekandaba, 2019) seems an important step for the public sector buy-in into a product. Yet questions arise as to why the public sector itself has resigned from the capacity to independently develop its own products, in spite of the challenges of lock-in and negative outcomes for citizens that have marred its previous attempts to fully outsource functions (Breckenridge, 2019).

Multi-stakeholder product development helps to ensure a variety of perspectives can be embedded in development, but for the public sector to provide proper oversight and effective implementation of a technological product intended for development purposes, there must be internal capacity to do so. When WhatsApp raised in its Heads of Argument the challenge that users of the channel could not be sure who they were engaging with through the shared platform, they were highlighting a problem that has actually emerged in the outsourcing of the social protection function previously: social obligations that exist for the public sector are harder to place on private sector entities given challenges to assigning responsibility (Razzano, 2020c); and this accountability challenge is only expanded when there are transparency problems as well that are inherent in blurred lines of responsibility. Consider for example – when the Minister of Social Development was questioned in Parliament who GovChat, as the main implementing partner of a social function, was working with - the Minister answered:

> "a) SASSA is not privy to the partnerships which GovChat has and who they work with, but is aware that GovChat is also providing data service platforms to COGTA (since 2017) and the Department of Health.
>
> b) SASSA is not privy to the role that other partners play" (*Question NW973 to the Minister of Social Development*, 2020).

In the previous public-private partnership between SASSA and CPS in the delivery of social grants, the courts were compelled to extend constitutional obligations on CPS as a private sector actor engaged in the delivery of public obligations given the seeming exploitation of citizens that resulted (but also

due to the financial exploitation that could arise from unfettered access to vulnerable communities with little other choice) (Breckenridge, 2019).[18] Yet, the ability of the courts to in an *ad hoc* manner extend obligations, does not adequately deal with business incentives that can often contradict public development objectives – exemplified by CPS's former CEO Belamant stating expressly in concerns raised about the exploitation of beneficiaries: "We're not a government, we are a company. We work for profit" (Pather, 2017). This misalignment need not be inherent to public-private partnerships, but they should be considered in planning the forms of policy interventions that may facilitate the delivery of 'good' AI in these contexts. Foundationally, it is important that POPIA creates data protection obligations on both public and private sector actors. Yet, there are other forms of accountability that may be important in the implementation of AI that may not be as clearly extended – such as in decision-making.

It is also important in these relationships to consider who's interests 'trump'. In explaining WhatsApp's position there is a telling paragraph in the Applicant's Heads of Argument:

> "The gist of Mr Supple's email was that the *"current structure"* of GovChat's business was in conflict with WhatsApp's terms of use which, according to him, require that each government department or entity utilising the GovChat platform would be required to open their own WABA (i.e., deal directly with Facebook / WhatsApp). He also indicated that #LetsTalk would no longer be able to engage in any messaging services on behalf of *"any government agencies or other third parties"* – i.e., that the GovChat platform could no longer operate via WhatsApp's Business API. **He concluded by noting that once the relevant government entities had established a direct relationship with Facebook / WhatsApp, they could continue to work with GovChat as a *"strategic advisor"***. In sum, Mr Supple was clear that the applicants would henceforth be denied access to the WhatsApp Business API" [Emphasis added]. (Farlam SC & Kelly, 2020)

In using a private sector platform to delivery public communications, public sector entities potentially surrender their autonomy in decision-making and make themselves subject to private sector policies. This is an important dynamic to consider.

While these relationships may be complicated, the ability for GovChat to so quickly respond in its development to the COVID-19 crisis is no doubt in part because they are able to drive the development of the product outside bureaucratic constraints (Malinga, 2020b). In fact, the structure of bureaucracy's may themselves bring about different forms of accountability challenges, as Arendt has famously noted:

> "The greater the bureaucratization of public life, the greater will be the attraction of violence. In a fully developed bureaucracy, there is nobody left with whom one could argue, to whom one could present grievances, on whom the pressures of power could be exerted. Bureaucracy is the form of government in which everybody is deprived of political freedom, of the power to act; for the rule by Nobody is not no-rule, and where all are equally powerless we have a tyranny without a tyrant"(Arendt, 1970).

Certainly, GovChat is seeking to position themselves as a collaborative, socially focussed private sector company. And it seems certain that the delivery of technology-centred products will heavily focus public sector partnerships with the private sector, in differing formations. It is interesting to note however that Motty Sacks – the investor and now co-owner in GovChat – was a founder and

[18] See *AllPay Consolidated Investment Holdings (Pty) Ltd and Others v Chief Executive Officer of the South African Social Security Agency and Others* 2014 (4) SA 179 (CC).

Chairman of Net1 (Buthelezi, 2020). He did however leave Net1 prior to CPS receiving the national SASSA social delivery tender. The point is not to imply that GovChat is necessarily a "new CPS by another name"; instead, it is that there is a limited pool of technology companies and expertise from which the South African public sector is choosing its partners, which incrementally increases the risks of "lock-in" that South African competition, and other, regulators will need to be highly cognisant of in trying to help balance public and private interests (Breckenridge, 2019).

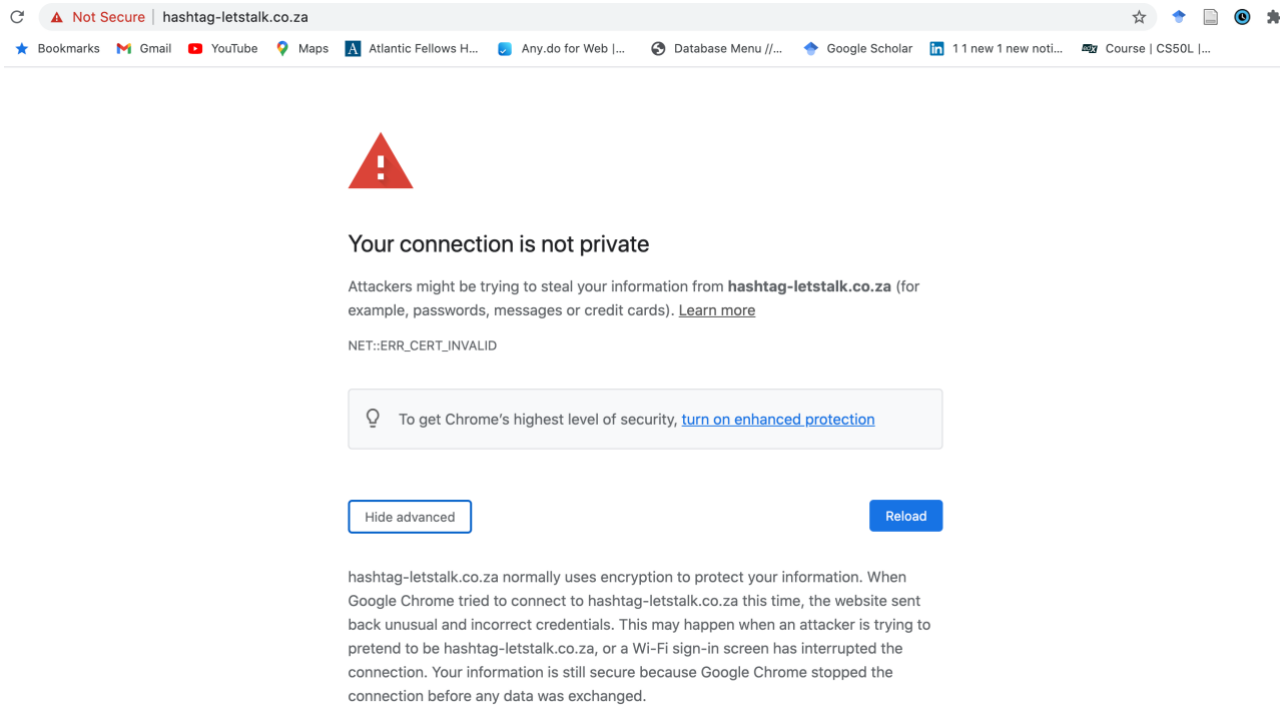
13.4 Risks and harms

Considering specific risks and harms that emerge in the South African case study outside of issues already flagged in both the definition of the case study and the rest of the analysis (particularly in the inequality and exclusions section), it is worth re-highlighting the particular risks that can emerge from a data protection perspective – particularly in a context where both the nature of the public-private partnership that can be obfuscating, and weaknesses evidenced in the leading partner (GovChat's) processing practices, are already indicated.

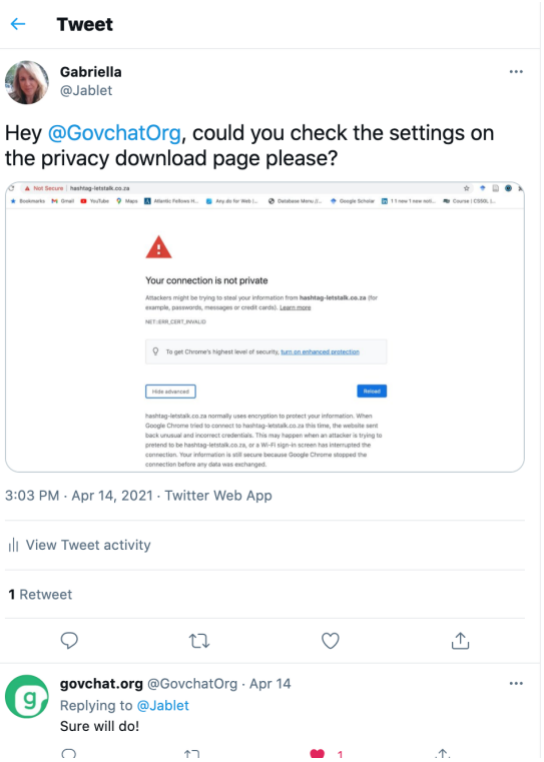
Data protection

WhatsApp itself questioned in its Heads of Argument how data protection can be assured in the context of an application that's purpose and use pivots regularly (Wilson SC & Berger, 2021). They raise the challenges for users in identifying responsible parties in the managing of the use of the WhatsApp channel given GovChat's role as a conduit for government communications (Wilson SC & Berger, 2021). Though these issues are raised in the context of the competition challenge, it is interesting to consider how GovChat might manage the two issues of both accountability, and purpose specification (two central lawful processing grounds in POPIA), given their current business model.

And unfortunately, it is difficult to determine these strategies given the unavailability of the privacy policy for the GovChat WhatsApp channel. When you try and access the privacy policy from the GovChat WhatsApp channel (which remember facilitates the SRD instance as well) the following message is received:



In spite of raising this issue directly with GovChat through the Twitter feed, over a week later the error had still not been fixed:



In this context, it is important to remember the kinds of personal data (including personal communications) that is being shared, received and processed through GovChat. Think, for example, of the personal data required for the SRD grant, which includes the applicants:

- Identity Number or Department of Home Affairs Refugee permit number,

- Name and Surname,
- Gender and Disability status,
- Contact details, including cell phone number, and
- Residential Address.

The above paragraphs outline the data protection ramifications of the GovChat WhatsApp channel itself. As the functions expand, too, digital identity will begin to be implicated additionally. The online SRD portal was amended to create an API, which facilitated authentication of applications with existing data sources on identity held by government (M. of P. Masango, 2020). This is being done in a context in which the DHA itself has already noted challenges in the statutory frameworks to facilitate data sharing for identity authentication:

> "[The Identification Act and Alteration of Sex Description Act] are key legislation that regulate how personal data that is hosted in the DHA identity management systems is handled. The legislation **needs** to be amended to regulate handling personal information in line with the Constitution and the POPI Act. The current practice of dumping the department's data on other government systems is contrary to the POPI requirements" [Emphasis added] (Department of Home Affairs, 2020b).

This is indicative that both the private sector and public sector actors involved in the implementation of GovChat need to get all the formal and practical processes better aligned to the new data protection order that POPIA is seeking to create as a matter of urgency.

In considering what the implications for AI might be, it is worth reiterating again that the actual AI implementation on the project seems threadbare and only relates to natural language processing and knowledge representation (Stahl, 2021). This places a re-emphasis on the need to prioritise the foundations for sound data processing as an urgent first step. In the medium and short-term attempts to consider AI law and regulation should focus on the specific applications of the technologies first (Stahl, 2021). However, the data processing foundation also point to an important regulatory emergence – the need for regulators that are adequately capacitated to deal with technological realities (Klaaren, 2021a; Stahl, 2021).

Social development and financialisaton

Conceptualising the legal challenge that has been central to the case study as a competition case brings an important question to the fore: in what way might GovChat and WhatsApp actually be competing? GovChat has numerous Government clients, but streamlines all their needs through its centralised communications channels. By creating requirements that each Government department apply directly for its own Business Account on WhatsApp, GovChat suggested the intention was to essentially poach its business clients (Farlam SC & Kelly, 2020). Yet, this still not adequately seems to provide a *commercial* interest for WhatsApp. In this regard, two sections of each of the Heads of Argument (read in the context of the historical developments in social development outlined above) could be of interest. In para 32 and 64 of GovChat's Heads of Argument they claim:

> "[32] [T]he respondents do not address, or thus dispute, the allegations in the founding papers that Facebook **itself has ambitions to render payment processing services in future via WhatsApp** (as it is doing in other emerging markets such as Brazil and India), and that it has ambitions to *inter alia* use WhatsApp to distribute payments on behalf of government – thereby potentially placing it in competition with the GovChat platform.

> …
>
> [64] Despite GovChat, through Mr. Jordaan, having expressly drawn Facebook's and WhatsApp's attention to the comparable services offered by Praekelt, Aviro Health and Internet Filing in its letter of 2 August 2020, and Facebook having promised to revert with respect to the contents of that letter, Facebook has never addressed these contradictions and anomalies...These objections have come despite the fact that GovChat's assistance to SASSA with regard to social relief of distress grant applications is essentially a continuation of the earlier arrangement between Praekelt, SASSA and the DOH (evidently acceptable to Facebook), **which was discontinued when Praekelt wanted SASSA to provide it with information regarding its "*payment capability*"** and the distribution of grant payments – which SASSA was uncomfortable with providing. (SASSA then approached GovChat, which agreed to assist SASSA immediately on a *pro bono* basis in addition to digitizing the grant application process)" [References omitted and emphasis added] (Farlam SC & Kelly, 2020).

These two paragraphs raise a likely understanding. In para 64, GovChat is implying of their previous technology partner Praekelt (who were later replaced by GovChat's new funding partners technology firm, Synthesis software) and WhatsApp as both having an interest in payments on behalf of government. This is in spite of the fact that GovChat itself does not currently issue payments through the SRD iteration, but rather allows for applications for the SRD. In seeking to rebut this perspective, WhatsApp notes in para 132-133:

> "Notwithstanding his acknowledgement that he has 'no information as to Facebook / WhatsApp's plans for payments in South Africa specifically', Mr Jordaan nevertheless baldly asserts that '[i]t is a reasonable inference that the respondents are keenly aware of the potential of South Africa as a highly attractive emerging market for mobile payment solutions and, in particular, the opportunity for access to the social grants payments by government.'
>
> The allegation regarding the potential for future competition between GovChat and WhatsApp is therefore underpinned by nothing more than conjecture and speculation; there is simply no evidence to sustain the allegation that the parties compete for business or are likely to do so in the foreseeable future".

WhatsApp does not deny the claim (and needn't), but states it is conjecture. Yet, it is widely understood that part of Facebook's acquisition of WhatsApp must be to better monetise its business model in some way – and facilitating payments through the application will probably be an eventual pivot (Wagner, 2020). It is notable too that – in spite of, at this stage, quite a broad range of partners in government and outside – GovChat itself frequently refers to protecting its businesses with SASSA, in particular. Yet GovChat has offered the WhatsApp channel to SASSA for free – begging the question how GovChat itself might also pivot its business model for revenue (one development of course has been their launch of a private sector focused product #LetsTalk) (*Question NW973 to the Minister of Social Development*, 2020). It is feasible that simply having access to such vast amounts of consumer (citizen) data for training its AI and refining its business model may be incentive enough. Yet, the intention to move to payments was cited by GovChat itself as central to the investment of its funding partner, Capital Appreciation, stating in response to the investment:

> "Furthermore, GovChat will use the funds to scale its digital payments technology, which it says will facilitate 0% transaction fees for social-good and small and medium enterprises across SA" (Mzekandaba, 2019).

The size of the social development programme in South Africa means it will continue to be a site for private sector competition of market share etc., but also that it will continue to be an important site for considering the data protection aspects of biometric and digital identity. These moves will incredibly expand on the potential risks involved in the AI iteration, not just in relation to data protection but also in relation to the potential exclusion from services and other risks that may be associated to automated decision-making within a grant's distribution programme.

13.5 Human rights

While many of the broader human rights reflections considered under the Ghana case study bear reflecting on in the South African context too, the robust South African constitutional framework and jurisprudence environment are able to provide rich context for forwarding development ambitions in the country. South Africa's Constitution protects the right to privacy in section 14:

> "Everyone has the right to privacy, which includes the right not to have
>
> a. their person or home searched;
>
> b. their property searched;
>
> c. their possessions seized; or
>
> d. the privacy of their communications infringed".[19]

The direct reference to communications privacy has been expanded to include informational protection; and is a relatively direct constitutional reference to information privacy that many regional Constitutions do not share (often privacy is merely captured as a form of property right). South Africa's constitutional regime is based on 'no fault'; in other words, once a breach is established, there is not a requirement to demonstrate fault (McQuoid-Mason, 2014). The essential structure of the constitutional provision is to outline the methods by which privacy might be infringed i.e., through search, seizure, or communications interference, rather to centre on what is the remit of 'private' (this remit has emerged through case law). In spite of these organic expansions of the informational components of privacy from the Constitution, POPIA has been drafted to give effect to the constitutional right. It is within this frame that the challenges experienced in relation to data protection, outlined earlier under 'Risks and Harms', need to be understood. While the individualised understandings of privacy may be insufficient for a fall understanding of privacy (Razzano, 2021), the IRSA will be an essential avenue for individuals seeking to protect their rights in large-scale data collections that may form a part of the evolving social protection paradigm.

Yet, the intersections between social protections and AI in South Africa highlight other important rights not least of all rights to access to information (section 32) equality (section 9), citizenship (section 20), and social security (section 27). Any limitation of rights will also be subject to establishing justifiable limitations as contained in section 36. This is an important context – in many international jurisdictions, socio-economic rights like security are not justiciable – which means South Africa's human rights regime provides important broad protections to its citizens (and others). This is an important framework for understanding the future of AI implementation in South Africa – but there are echoes of the human rights regime (and the Constitution's status as supreme law of the land), which informed the 'public interest' considerations highlighted by the Competition Commission in its

[19] Constitution of the Republic of South Africa, 1996, section 14.

Tribunal decision under this case study. Human rights imperatives are streamlined within the broader legal order.

Reflection on the specific risks and harms additionally triggers consideration of the right to administrative justice in the emerging technological order (Razzano, 2020c): expanding the remit of administrative justice – and who bears positive obligations under its regime – will be an important consideration in a context such as the one described, where the exercise of public functions through private entities (or significantly aided by private entities) can sometimes create accountability challenges.

14 Key Case Study Findings

The GovChat case study is an example of a private sector led initiative, that collects identity information for helping to process social grants and uses AI for natural language processing. It does not collect biometric data, but does collect national identity numbers, though the historical context provided on biometric data in relation to foundational identity has helped unpack dimensions of opportunities and risks within the AI and data environment. Like Ghana, this project was more reflection of functional identity than foundational identity.

- South Africa has centralised biometric and national identity ambitions. However, digital identity is largely demonstrated in functional instances. The foundational identity project, however, does demonstrate the historical challenges in centralising identity given Apartheid and colonial legacies, and also the importance such projects can have for ensuring adequate social development and service delivery through 'visibility'.
- A more traditional understanding of AI and biometric and digital identity can be seen in how AI helps facilitate authentication (as seen in the Ghana case study that accompanies this case study). However, the social development context helps to highlight how lessons from South Africa's historical biometric and digital identity projects helps set the stage for the broader implementation of AI across development projects, and the centrality that public-private partnerships will play as a political nexus.
- The implementation of AI on social development contexts is still nascent. There is, however, a strong necessity to drive lawful data processing practices across involved public and private sector actors ahead of broader AI implementation, particularly given how personal data is the base of biometric and digital identities. Looking forward to expanded data collection exercises as part of a) expanding social development programmes, b) the growth of data-hungry AI, and c) centralising national identity projects, do the historical examples actually demonstrate that South Africa's 'new' POPIA frames may be insufficient? In particular, how will collective interests potentially be protected in the face of private sector and public sector mass collection exercises? The GovChat case study demonstrates how the good practice is still only emerging.
- The South African case study demonstrates how a frontier for conflict will inevitably arise in relation to competition, with both local and global dimensions, when looking at the incorporation of technologies in public development. While the Competition Commission has demonstrated a willingness to consider the public interest in providing interim relief to GovChat in its dispute with WhatsApp, the case importantly raises how the 'source' of competition appears to be a desire to have access to SASSA's beneficiaries service distribution. This too re-emphasises the importance of data protection.

- GovChat has had numerous iterations (to a point where it is quite challenging to even separate these iterations out). This is in fact some of the criticism by Facebook of GovChat's practices. In the context of POPIA, it is very interesting to consider how the *practice* of innovation, and the culture of 'pivoting', is challenged by the regimented frames provided by data processing laws like POPIA (consider for instance processing requirements for "purpose specification" and "accountability" discussed under the 'Legal' section).
- Whilst it is difficult to extract details on the form of the AI technologies (and importantly, the dynamics of the data underscoring them), this in itself is a finding: the proprietary nature of technological development in AI (and not just 'black box' technologies themselves) will continue to make it a challenge to monitor the social and political dimensions of these products. In fact, in this case study it appears as if the role of AI elements may be overstated.
- There are many forms of exclusion that arise from both poor data governance practices, public-private partnerships, and potentially even AI in terms of decision-making in relation to social protection. Yet, these must be understood in terms of the current forms of lived exclusion that occur because of failing logistical systems, and existing gaps in terms of law and regulation (as discussed under the 'National digital and biometric identity').

Part E: Thematic Synthesis

15 Thematic discussions and conclusions

15.1 Limitations across case studies

As reflected on in the 'Case Study Limitations', neither of the case studies deals strongly with foundational identity and rather stand chiefly as functional identity systems (Bhandari et al., 2020). Further, the South African case study wasn't centrally an identity project. Nevertheless, there are significant lessons in the attempts to implement functional identity that extend to foundational identity. And in fact, this relates to a finding in the research (discussed below).

Whilst it is difficult to extract details on the form of the AI technologies (and importantly, the dynamics of the data underscoring them), this too is in itself a finding: the proprietary nature of technological development in AI (and not just 'black box' technologies themselves) will continue to make it challenging to monitor the social and political dimensions of these products, particularly given the role private sector companies are playing in the development of public sector solutions.

15.2 Foundational national identity

Both in Ghana and South Africa the case studies were largely examples of functional identity systems, though GovChat did collect national identity numbers. This could have resulted of course from poor case study selection, but it is worth noting that the case selection was based off a mapping of projects that specifically sought to identify components of civil and national identity. Instead, it is the nascent stage of AI – but also the state of foundational identity systems – that is implicated. As an interview with a product owner in the field of biometric and digital identity in Africa noted,[20] the separation from foundational projects for many private sector and social entrepreneurship initiatives is intentional for those creating development solutions: foundational systems in Africa can be unreliable, and partnerships with the state at that level challenging to maintain consistently to ensure product quality. The comprehensive histories of the Ghanaian and South African national identity systems both support this interpretation.

15.3 Digital economy and innovation environments

Both case studies saw development technologies being led by private sector initiatives, and in both cases the foundations of the companies were supported through additional start-up funding. This speaks to the realities of innovation companies and their costs, raising the question of how policies to foster local innovation adequately address funding, access to capital, and access to alternative funding sources. This is a theme that will be considered under other aspects of the project.

15.4 AI and visibility

Both case studies highlight the importance that visibility, through sound biometric and digital identity, plays for the delivery of social and financial services to the public. This overarching benefit must always be placed at the forefront of narratives that also highlight the particular risks that can emerge due to the vulnerability of low digital literacy citizens being the subject of digital identity

[20] The interview was conducted 30 April 2021, though the respondent wished to remain anonymous.

campaigns. These immediate benefits must also be used to consider dynamically the ability of citizens to exert real agency within these data collection exercises (Razzano, 2021). Whilst this caveat is especially true in the context of foundational identity systems, the context of these functional identity systems helps to highlight how transparency is an important partner to mitigating against the peculiar risks of the context.

15.5 Lack of transparency

A challenge implementing the research has been the lack of information available that has allowed for a real deep-dive into the technology actually deployed – but this is, as well, a finding. There are two dimensions to challenges in transparency that emerge from the case studies:

- An unwillingness to share information that may have commercial value, but would nevertheless allow for some consideration of the extent of AI actually incorporated (related to both BACE-API and GovChat); and
- A lack of transparency born of the nature of agreements between public and private partners that would better provide for investigations into the nature of the personal data (and personal data processing) that underscore the identity technologies (again related to both case studies).

This requires both practical and legal mechanisms for enhancing transparency in the biometric identity space. Certainly, provisions in data protection laws that allow for data subjects rights of access are important, but – as the South African context alluded too – it also highlights how important intersections with other human rights, such as rights of access to information, will be in creating an enabling environment for the implementation of good biometric and digital identity in Africa, as well as good AI.

Proactive preservation of rights in the design of a product is a practical manifestation of this issue. The classic example is 'privacy by design', the approach taken when developing digital technologies and systems by which privacy is incorporated into technology and systems by default during the design and development process (Cavoukian, 2009). Within the transparency context, though, this will be done by ensuring in the AI product design process that things like 'black box' decision-making are technologically prevented (Black & Murray, 2019; Pasquale, 2015). Design solutions might be initiated by designers themselves, but might also be positively prescribed in regulation.

15.6 Risk assessments

A particular challenge, which emerges from limits in transparency is the inability to then properly assess chief risks that may be important for planning policy intervention, and how – if at all – those risks have influenced decision-making. As demonstrated by the GovChat case study, a lack of transparency even in relation to implemented privacy policy protection (let alone the realities of the data processing practices) may contribute to heightened risks for citizens participants in biometric and digital identity systems.

There are of course direct challenges that emerge in the monitoring of the implementation of identity projects in the context of a lack of transparency. And while both case studies were private companies, as companies move closer to the distribution of public services, the associated transparency imperatives should only increase (Razzano, 2020c).

There is a specific issue, which also emerges in the AI regulatory context and is supported by the findings of this research: the emerging, consistent calls for the institution of risk assessments prior to

the development of a product and after its deployment to ensure 'good' AI in design *and* outcome (Crawford & Calo, 2016). Yet again, it seems clear advances in transparency will be needed to facilitate oversight through these kind of design processes to ensure accountability.

15.7 Data privacy plus+

While both case studies supposedly incorporated AI, the nascent stage of solutions highlights how the priority should remain instituting sound data processing governance as a necessary (but insufficient) regulatory measure for supporting good AI. This is not only because of the AI itself, but also because both case studies demonstrate that the emergence of data governance frames are not necessarily yet satisfactorily implemented.

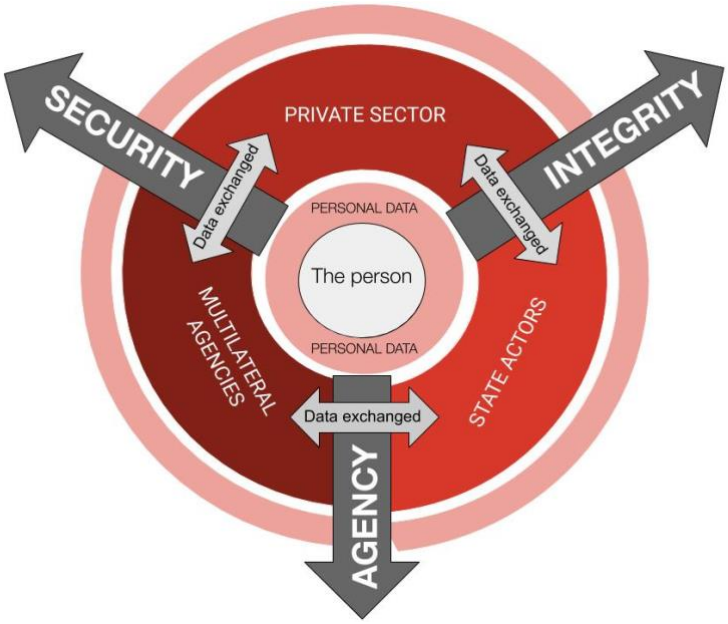


Figure 3: Modes of constructing digital identity © Razzano 2020

Looking back to the framing diagram, which helps to outline data processing principles, centring the concerns on the subjects themselves provides a tool for understanding particular sites of risk in the data context. And of course, if challenges are identified, a further dimension then arises in relation to accountability and recourse.

15.8 Public sector capacities

While acknowledging again the challenges in considering a full scale of public sector issues given both case studies were ancillary to foundational digital identity, both cases highlight how the private sector is emerging as an important designer and implementer of public sector identity solutions. While Historical considerations of the South African case study helped highlight some of the *risks* that might emerge when these forms of partnership act as 'digital hegemonies' (Razzano, 2020d), there is also a direct issue in the inability of the public sector to embed capacity internally. This renders the public sector heavily reliant on such partnerships, especially vulnerable to lock-in (Breckenridge, 2019), whilst also bringing into question their ability to assert public sector imperatives within these relationships to the full benefit of citizens.

15.9 Digital hegemonies and competition

The litigation at the centre of the South African case study squarely alerted the research to very direct intersections with competition concerns, staged on a global-local intersection. It is worth considering too the technology context: in Ghana and South Africa the same actors (Net1) dominated biometric projects (and resulted in similar criticisms of corruption). A limited pool of technological capacity will only grow competition challenges. It also implicates the need to facilitate broader innovation environments not just to grow private sector benefits, but also to enable the development of AI technologies of direct benefit to public sector development as well.

16 Recommendations

16.1 For Future Research

- In terms of broader future research, the case studies do raise the importance of creating a research framework or methodology for helping to define how functional and foundational do and don't correspond, for shared learning.
- In terms of instituting future case studies in this area, significant energy should be placed on outlining the actual data processing practices that underscore biometric and digital identity technologies.
- In terms of policy intervention areas, guidelines for the institution of socio-economic risk assessments of biometric and digital identity project should be outlined.
- Identity projects arise within a particular social and political history of exclusion for many African populations. This will need to influence what we consider useful interventions to be, but also means it will be a reality that a significant area of AI technology will relate to identity authentication processes in the near future (which means creating norms and standards for these kinds of activities should be a research priority).
- As more AI technologies are developed, a strong focus in the research should be considering the specific *type* of AI technologies being implemented and the specific *types* of data underpinning it – risk assessments should be technologically specific.

16.2 For Policymakers

- Data governance frameworks are a priority foundation for the implementation of biometric and digital identity programmes.
- Foundational identity projects will need to constructively coalesce with functional identities in order to reap the benefits of good AI.
- All policies must be established within a considered analysis of the full extent of intersecting digital inequalities.

16.3 For Lawmakers

- Regulatory interventions should consider the extension of transparency mechanisms in the context of biometric and digital identity, in particular.
- The expansion of social obligations for assuring good AI must be assured given the role of the private sector in the delivery of public goods and services.

16.4 For Technologists

- The implementation of socially focused identity projects should remain authentically connected to their public good purpose.
- Socio-economic risk assessments should be implemented prior, and post, the implementation of biometric and digital identity AI technologies.

Annexure A: Research Design and Methodology

1. Introduction

The research methodologies undertaken for each case study are provided for in more detail within the case studies below. However, the research methodology and approach for the thematic area as a whole can be outlined first.

2. Mapping

The specific case selected arose from a mapping of digital identity and BDI projects . For this mapping exercise, an initial list of possible projects was extracted from the World Bank "ID4D" Global Dataset.[21] Further case studies were then identified through desktop review (which was also used to expand on the original projects selected) with a focus on:

- digital identity,
- development, and
- artificial Intelligence.

A mapping structure was then created,[22] based on the initial literature review undertaken as 'Phase 1' of the research. While the framework for analysing digital identity systems provided for by the Centre for the Internet Society's "Governing ID: A Framework for Evaluation of Digital Identity" was considered while drafting the template, given its focus on the *evaluation* of such systems (an exercise that will inform the later analysis under our selected case studies), and its limitation was to digital identity system, it was not replicated in its entirety (Bhandari et al., 2020).

The map was created in line with two objectives. The first was to try and inform consistency along the different streams of research being undertaken simultaneously (see further 'Project Context' above). The second was to help extract details relevant for consideration within the exploration of digital and biometric identity projects, in particular.

Of the fourteen country projects that were taken from the database, none had significant evidence of incorporating AI elements. Identity programmes that were associated to AI, instead, emerged from the later supplementary desktop research.

In the case studies, which included both digital identity and AI functions, all except one of the examples incorporated AI-based identification within digital systems for authentication and/or security functions. Looking at the mapping data – in a manner different to the Surveillance Mapping Data – when AI projects are found, they often incorporate domestic technologies, rather than just the importing of technologies from the US and/or China as is often posited in the narratives (though of

[21] The dataset can be viewed here: https://id4d.worldbank.org/global-dataset

[22] The map is available here: https://docs.google.com/spreadsheets/d/1WSDdc78GbIWk2rdnYcm_kA7vyGzxPTSl2Twx5En4E5A/edit?usp=sharing

course what components of the systems may have been imported will only be revealed through the in-depth case studies). This is perhaps due to their civil and national registration functions, which are pre-existing and being adapted, rather than being introduced independently.

2.1 Lessons from the mapping

There were challenges in seeking to identify actual case studies of identity systems that feature AI-based technologies, deployed in Africa. This may be because much of these are in the exploratory phases, or are not readily in the public domain. A chief example, however, of where AI and Digital Identity systems align is in systems that incorporate "Smart Biometrics".

Another important issue that emerges was between what can be referred to as Digital Identity with a big "DI" (directly related to national identity programmes) and digital identity (as a functional identity), more broadly (Bhandari et al., 2020). Of course, there are a multiplicity of digital identity types (with authentication methods) that run across digital services; however, this project was focused on Digital Identity as related to national civil registration processes, primarily. Digital Identity is of course connected to state-driven development agendas, however digital identity and financial inclusion, in particular, can also pose development challenges. This difference was born in mind in the cases selection. This finding in the mapping is not, however, investigated further in the case studies. The lack of sufficient active AI overlaps meant that the strict definitions could not necessarily be abided by in case study choices.

2.2 Criteria for Case Selection

Based on the broader project objectives, but also in response to the initial phases of the research, the following criteria were considered in selecting the case studies (applied below):

A. Relevance to broader research;
B. Relevance to digital and biometric identity system challenges;
C. Relevance to the regional context, in particular; and
D. Variety across selected case studies.

Considering the (A) criteria was particularly important as a precursor, especially when considering that (as seen above) most cases of AI are only being evinced as either authentication or security functions (and 'overlaps' with the Surveillance theme outlined above). These criteria were then used to establish the two chose case studies as the focal point from the mapping results.

3. Ghana Case Study Methodology

3.1 Research design

Chiefly designed as explanatory case study research (and building off the research methodology described in section B), the research leveraged qualitative design methods with a strongly focused political economy lens (Yin, 2018). Given the analytical needs, the relevant social, technological, economic, environmental, and political context should be outlined (Szigeti et al., 2011).

3.2 Data collection

A variety of data collection activities were incorporated, with secondary data chiefly sourced through an extensive literature review (see the Reference List outlined in detail below). Interviews were

conducted with different interviewees, but these largely only informed analysis as secondary sources, rather than serving as primary data.

In terms of primary data collection. The following data sources were reviewed:

- Conference attendance which allowed for primary data collection from the BACE-API team (including the Fintech Circle, xAI Conference, 9 December 2020);
- Promotional materials supplied after direct information request to BACE-API;
- Social media analysis (including review of the BACE-API website, Twitter Feed and LinkedIn channel).

As a note on the veracity of social media content as a source of primary data, while it is marketing materials of a company and thus must be approached with caution in terms figures etc., it can be interpreted very strongly as representative of the *intended* presentation of a company or individual to the public.

3.3 Analysis

The analysis of all these research questions was done with a gendered and political economy lens. Strongly informing the political economy analysis were research questions on public/private partnerships and power distributions; the imperatives of development economics, in particular; state capacity and capabilities; and global governance and multistakeholderism. Chiefly, however, the analysis focused on answering the outlined case study research questions.

4. South Africa Methodology

4.1 Research design

Again, this was chiefly designed as explanatory case study research (and building off the research methodology described in section B), the research leveraged qualitative design methods with a strongly focused political economy lens (Yin, 2018). Given the analytical needs, the relevant social, technological, economic, environmental, and political context should be outlined (Szigeti et al., 2011).

4.2 Data collection

A variety of data collection activities were incorporated, with secondary data chiefly sourced through an extensive literature review (see the Reference List outlined in detail below). Interviews were conducted with different interviewees, but these largely only informed analysis as secondary sources, rather than serving as primary data. However, data from one interview was influential (see below). Conference attendance at the South African Journal of Human Rights COVID-19 issue conference included an extensive, but secondary, discussion on the GovChat instance (Klaaren, 2021b).

In terms of primary data collection. The following data sources were reviewed:

- Social media analysis (including review of the GovChat website, Twitter Feed and LinkedIn channel);
- Company documentation available on request through the Companies and Intellectual Property Commission user portal;

- Extensive review of parliamentary records (equivalent to Hansard records) made openly available through collaboration with the National Parliament on the Parliamentary Monitoring Group (https://pmg.org.za/);
- Applicant and respondent papers submitted to the Competition Commission in GovChat and Another / WhatsApp and Another urgent interdict hearing;
- Expert interview - on 30 April an interview was conducted with a civil society product owner working in a company that works on functional digital identity within the health sector. The interviewee requested to remain anonymous

As a note on the veracity of social media content as a source of primary data, while it is marketing materials of a company and thus must be approached with caution in terms figures etc., it can be interpreted very strongly as representative of the *intended* presentation of a company or individual to the public.

4.3 Analysis

The analysis of all these research questions was done with a gendered and political economy lens. Strongly informing the political economy analysis were research questions on public/private partnerships and power distributions; the imperatives of development economics, in particular; state capacity and capabilities; and global governance and multistakeholderism. Chiefly, however, the analysis focused on answering the outlined case study research questions.

Annexure B: Full research questions

State of Digital ID and Biometric System

- What stage are the rollouts at?
- Which actors are driving and implementing the process (government, private sector, civil society; domestic, foreign, global; demographic diversity, etc)?
- What are the motivations of these actors?
- What are the historical and political factors of relevance to the role of these actors in the system?

Socio-technical systems

- What technologies/technological systems are being used?
- Where do they come from/whose knowledge was used to design the system (e.g., domestic v foreign sourced)?
- What is the AI component of these systems?
- Are they being integrated into existing ID systems or established as new systems?
- What data is collected, how and with what permissions?
- Who collects the data?
- Who owns the data/databases?
- Who has access to the data?
- How is data stored and shared?
- Who is captured and who is not captured?
- What are the pros and cons of being or not being captured?
- How adaptable are the systems to future technological developments?

Uses

- What purposes are the systems being used for (positive and negative)?
- Who is using them?
- Are they mandatory or elective for individuals?
- Where are the dominant uses cases appearing (countries, regions, sectors, industries, etc)?
- What are the possible political, social and economic forces that are driving/impacting these use cases?

Regulatory frameworks

- What regulatory frameworks are in place/being put in place to govern the systems?
- What rights and responsibilities do they address?

- What technical frameworks are in place/being put in place to support the regulatory frameworks?
- Are there any existing regulatory or technical frameworks that run counter to or contradict the principles of the new systems?

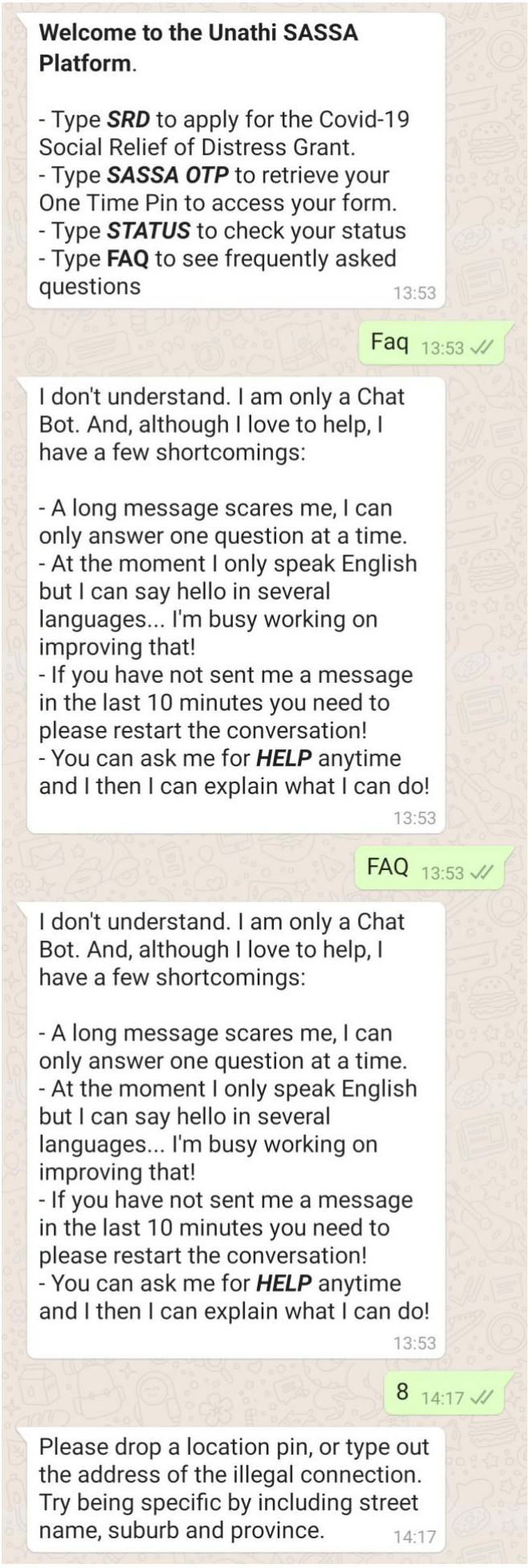
Potential positive impacts

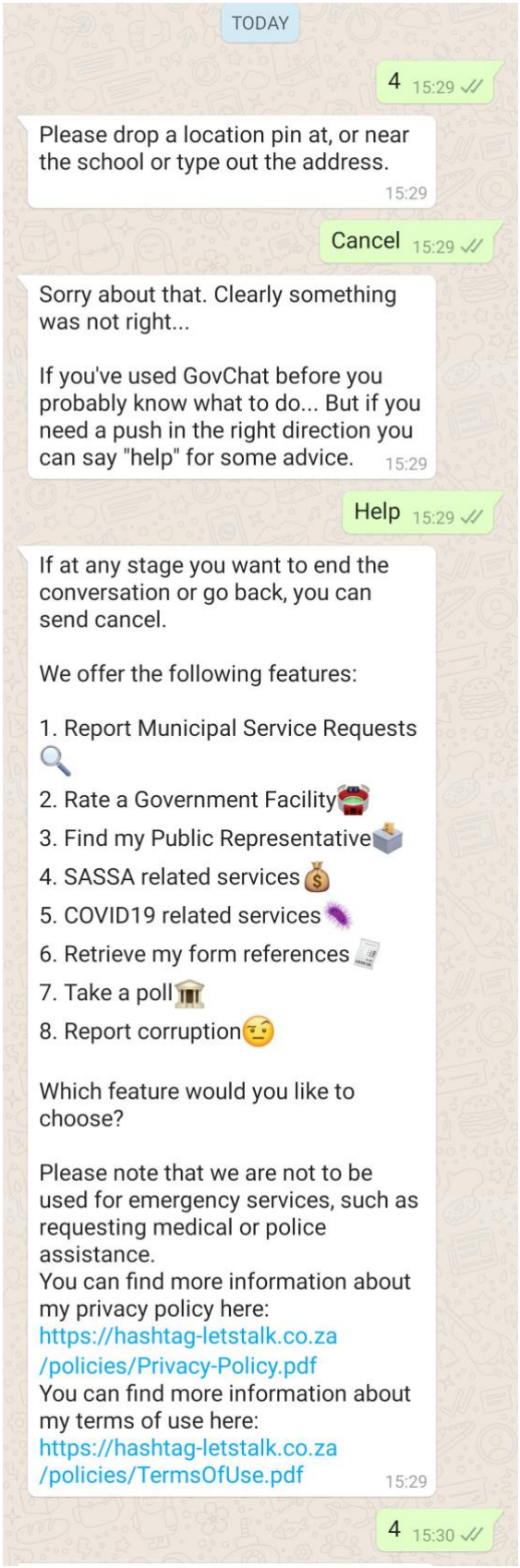
- What benefits are associated with the systems/use of the systems, particularly from a development point of view?
- How can digital ID augment access to government services as well as to financial services and access to the job market?

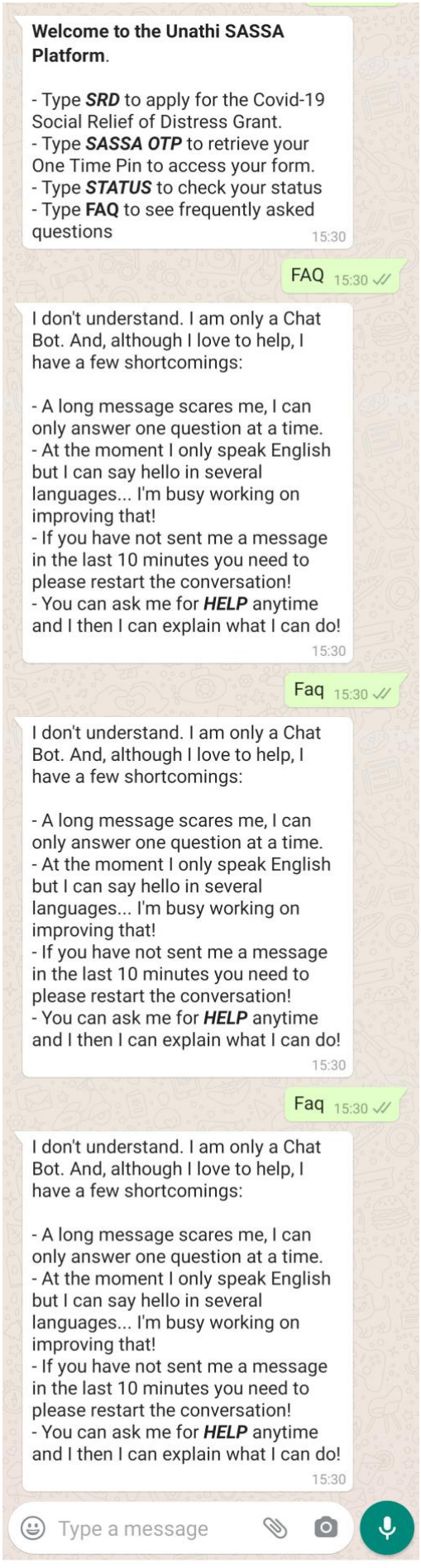
Potential risks/negative impacts

- How do existing social inequalities intersect with digital ID and biometric systems (gender, race, immigration status, others)?
- How do policy and regulation contribute to negative impacts, or negative environments that contribute to these negative impacts?
- How can systems be built to deliver social justice?
- What recourse is practical/possible to address risks as they occur?
- What policy or regulation is practical/possible to prevent the risks from occurring?

Annexure C: GovChat user journey


Welcome to the Unathi SASSA Platform.
- Type ***SRD*** to apply for the Covid-19 Social Relief of Distress Grant.
- Type ***SASSA OTP*** to retrieve your One Time Pin to access your form.
- Type ***STATUS*** to check your status
- Type **FAQ** to see frequently asked questions
13:53
Faq 13:53
I don't understand. I am only a Chat Bot. And, although I love to help, I have a few shortcomings:
- A long message scares me, I can only answer one question at a time.
- At the moment I only speak English but I can say hello in several languages... I'm busy working on improving that!
- If you have not sent me a message in the last 10 minutes you need to please restart the conversation!
- You can ask me for ***HELP*** anytime and I then I can explain what I can do!
13:53
FAQ 13:53
I don't understand. I am only a Chat Bot. And, although I love to help, I have a few shortcomings:
- A long message scares me, I can only answer one question at a time.
- At the moment I only speak English but I can say hello in several languages... I'm busy working on improving that!
- If you have not sent me a message in the last 10 minutes you need to please restart the conversation!
- You can ask me for ***HELP*** anytime and I then I can explain what I can do!
13:53
8 14:17
Please drop a location pin, or type out the address of the illegal connection. Try being specific by including street name, suburb and province.
14:17


TODAY
4 15:29
Please drop a location pin at, or near the school or type out the address. 15:29
Cancel 15:29
Sorry about that. Clearly something was not right...
If you've used GovChat before you probably know what to do... But if you need a push in the right direction you can say "help" for some advice. 15:29
Help 15:29
If at any stage you want to end the conversation or go back, you can send cancel.
We offer the following features:
1. Report Municipal Service Requests
2. Rate a Government Facility
3. Find my Public Representative
4. SASSA related services
5. COVID19 related services
6. Retrieve my form references
7. Take a poll
8. Report corruption
Which feature would you like to choose?
Please note that we are not to be used for emergency services, such as requesting medical or police assistance.
You can find more information about my privacy policy here:
https://hashtag-letstalk.co.za/policies/Privacy-Policy.pdf
You can find more information about my terms of use here:
https://hashtag-letstalk.co.za/policies/TermsOfUse.pdf 15:29
4 15:30


Welcome to the Unathi SASSA Platform.
- Type SRD to apply for the Covid-19 Social Relief of Distress Grant.
- Type SASSA OTP to retrieve your One Time Pin to access your form.
- Type STATUS to check your status
- Type FAQ to see frequently asked questions
15:30
FAQ 15:30
I don't understand. I am only a Chat Bot. And, although I love to help, I have a few shortcomings:
- A long message scares me, I can only answer one question at a time.
- At the moment I only speak English but I can say hello in several languages... I'm busy working on improving that!
- If you have not sent me a message in the last 10 minutes you need to please restart the conversation!
- You can ask me for HELP anytime and I then I can explain what I can do!
15:30
Faq 15:30
I don't understand. I am only a Chat Bot. And, although I love to help, I have a few shortcomings:
- A long message scares me, I can only answer one question at a time.
- At the moment I only speak English but I can say hello in several languages... I'm busy working on improving that!
- If you have not sent me a message in the last 10 minutes you need to please restart the conversation!
- You can ask me for HELP anytime and I then I can explain what I can do!
15:30
Faq 15:30
I don't understand. I am only a Chat Bot. And, although I love to help, I have a few shortcomings:
- A long message scares me, I can only answer one question at a time.
- At the moment I only speak English but I can say hello in several languages... I'm busy working on improving that!
- If you have not sent me a message in the last 10 minutes you need to please restart the conversation!
- You can ask me for HELP anytime and I then I can explain what I can do!
15:30
Type a message

Reference List

Addai, B., & Arthur, B. (2020). Ghana's Road to Cashless Economy: The E-Zwich Experience. *Journal on Innovation and Sustainability*, *11*(1). https://revistas.pucsp.br/risus/article/download/48838/pdf_1

African Union. (2020, December 9). *Preliminary Statement: AU Election Observation Mission to the Presidential and Parliamentary Elections in the Republic of Ghana*. https://au.int/en/pressreleases/20201209/preliminary-statement-au-election-observation-mission-presidential-and

Agyapong, D. (2020). Implications of digital economy for financial institutions in Ghana: An exploratory inquiry. *Transnational Corporations Review*, 1–11. https://doi.org/10.1080/19186444.2020.1787304

Aikins, E. (2020, June). *Compiling a new biometric voter's register amidst a pandemic.* Institute for Democratic Governance. https://ideg.org/publications/covid19-newbvr/

Allotey, G. (2018, October 4). Ghana loses $230m to cyber criminals – CID. *Citinewsroom - Comprehensive News in Ghana*. https://citinewsroom.com/2018/10/ghana-loses-230m-to-cyber-criminals-cid/

Arendt, H. (1970). *On Violence*. Harcourt Books.

Bailur, S. (2019, September 9). *Women and ID in a digital age: Five fundamental barriers and new design questions*. Medium. https://medium.com/caribou-digital/women-and-id-in-a-digital-age-five-fundamental-barriers-and-new-design-questions-79caa2a4acb8

Bajaj, N. (2020, September 21). Charlette N'Guessan: BACE tries to resolve the problem of identity fraud in Africa. *Platform Africa - Economic News for Emerging Market*. https://www.platformafrica.com/2020/09/21/charlette-nguessan-bace-tries-to-resolve-the-problem-of-identity-fraud-in-africa/

Baker, S. (2019). *What to look for in digital identity systems: A typology of stages*. Engine Room. https://www.theengineroom.org/what-are-the-stages-of-creating-a-digital-id-system/

Barocas, S., & Nissenbaum, H. (2013). Big data's end run around anonymity and consent. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, 44–75. https://doi.org/10.1017/CBO9781107590205.004

Bassier, I., Budlender, J., & Zizzamia, R. (2021). *The labour market impacts of COVID-19 in South Africa: An update with NIDS-CRAM Wave 3* [Wave 3]. National Income Dynamics Study.

Baylon, C., & Antwi-Boasiako, A. (2016). Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study. *Global Commission on Internet Governance Paper Series*, *44*. https://www.cigionline.org/publications/increasing-internet-connectivity-while-combatting-cybercrime-ghana-case-study

Besaw, C., & Filitz, J. (2019). *AI & Global Governance: AI in Africa is a Double-Edged Sword—United Nations University Centre for Policy Research*. https://cpr.unu.edu/ai-in-africa-is-a-double-edged-sword.html

Bhandari, V., Trikanad, S., & Sinha, A. (2020, January 22). *Governing ID: A Framework for Evaluation of Digital Identity*. https://digitalid.design/evaluation-framework-02.html

Black, J., & Murray, A. D. (2019). Regulating AI and Machine Learning: Setting the Regulatory Agenda. *European Journal of Law and Technology*, *10*(3). http://ejlt.org/article/view/722

Black Sash. (2018). *The SASSA / SAPO Card Swap Transition Monitoring Survey*. https://cbm.blacksash.org.za/survey-type/sassa-sapo-card-swap/south-africa/cycle/8/summary.pdf

Breckenridge, K. (2005). The Biometrie State: The Promise and Peril of Digital Government in the New South Africa. *Journal of Southern African*, *31*(2), 267–282.

Breckenridge, K. (2010). The World's First Biometric Money: Ghana's E-Zwich and the Contemporary Influence of South African Biometrics. *Africa*, *80*(4), 642–662. https://doi.org/10.3366/afr.2010.0406

Breckenridge, K. (2014). *Biometric State. The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge University Press. https://libcom.org/files/keith-breckenridge-biometric-state-the-global-politics-of-identification-and-surveillance-in-south-africa-1850-to-the-present.pdf

Breckenridge, K. (2019). The global ambitions of the biometric anti-bank: Net1, lockin and the technologies of African financialisation. *International Review of Applied Economics*, *33*(1), 93–118.

Breckenridge, K. (2020). *Biometric Capitalism*. The WISER Podcast | Wits Institute for Social and Economic Research. https://wiser.wits.ac.za/event/wiser-podcast

Buolamwini, J. (2019). Artificial Intelligence Has a Problem With Gender and Racial Bias. *Time*. https://time.com/5520558/artificial-intelligence-racial-gender-bias/

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Conference on Fairness, Accountability and Transparency*, 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html

Burchell, J. (2009). The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law*. https://www.ejcl.org/131/art131-2.pdf

Buruku, B. (2020, May 21). *Ghana Launches World's First Digital Finance Policy Amid COVID-19*. https://www.cgap.org/blog/ghana-launches-worlds-first-digital-finance-policy-amid-covid-19

Business News. (2018, October 2). *Ghana's cyber-security maturity at a formative level*. Ghana Web. https://www.ghanaweb.com/GhanaHomePage/business/Ghana-s-cyber-security-maturity-at-a-formative-level-Minister-689608

Buthelezi, L. (2020, June 2). *'Really unfortunate' that GovChat dragged into SASSA, CPS saga, says shareholder | Fin24*. Fin24. https://www.news24.com/fin24/economy/really-unfortunate-that-govchat-dragged-into-sassa-cps-saga-says-shareholder-20200602

Calandro, E., & Berglund, N. (2019, November 25). *Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC case*. Internet Governance Forum, Berlin, Germany.

Cavoukian, A. (2009). *Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices.* Information and Privacy Commissioner.

Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, & Unwanted Witness. (2021). *Chased Away and Left to Die*. Omidyar Network, Open Society Foundation.

Central Bank. (2020, February 3). *Central bank of the year: Bank of Ghana*. Central Banking. https://www.centralbanking.com/node/4690326

Cobbe, J. (2018). *Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making* (SSRN Scholarly Paper ID 3226913). Social Science Research Network. https://doi.org/10.2139/ssrn.3226913

Commission on the Fourth Industrial Revolution. (2020). *Diagnostic Report of the Presidential Commission on the Fourth Industrial Revolution*. https://www.itweb.co.za/static/misc/pdf/COMMUNICATIONS-AND-DIGITAL-TECHNOLOGIES-NOTICE-591.pdf

Couldry, N., & Mejias, U. (2018). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *SAGE Publications*. https://eprints.lse.ac.uk/89511/1/Couldry_Data-colonialism_Accepted.pdf

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

Creese, S. (2020). The Threat from AI. In D. J. Baker & P. H. Robinson (Eds.), *Artificial Intelligence and the Law*. Taylor & Francis.

Dagbanja, D. N. (2016). The Right to Privacy and Data Protection in Ghana. In A. B. Makulilo (Ed.), *African Data Privacy Laws* (pp. 229–248). Springer International Publishing. https://doi.org/10.1007/978-3-319-47317-8_10

Department of Home Affairs. (2020a). *Annual Report 2019/2020* [Annual Report]. https://drive.google.com/file/d/1cGvs_EUFhw-NOLOtGJGhe6ZoE1X_Q0ed/view?usp=sharing

Department of Home Affairs. (2020b). *Draft Official Identity Management Policy* (Public Consultation Version). http://www.dha.gov.za/images/PDFs/Draft_Official_Identity_Management_Policy_-_Gazette_Version_of_22122020.pdf

Donovan, K. P. (2015). The Biometric Imaginary: Bureaucratic Technopolitics in Post-Apartheid Welfare. *Journal of Southern African Studies*, *41*(4), 815–833. https://doi.org/10.1080/03057070.2015.1049485

ENCA. (2021, March 27). Govchat granted interim relief against Facebook and WhatsApp removing it. In *ENCA Live*. eNCA. https://youtu.be/kSe-W6hOua4

Falken, S. (2021, April 5). *GovChat: 'Facebook wants control of South Africans' data and how it is used'* [Interview]. https://www.capetalk.co.za/articles/413006/govchat-facebook-wants-control-of-south-africans-data-and-how-it-is-used

Farlam SC, P., & Kelly, L. (2020). *GovChat Proprietery Ltd and Another \\ Facebook Inc. And Another: Applicant's Heads of Argument*.

Fintech Circle. (2020, December 9). How will AI redefine the financial services industry? In *XAI Conference*.

Gandy, M. (2005). Cyborg Urbanization: Complexity and Monstrosity in the Contemporary City. *International Journal of Urban and Regional Research*, *29*(1), 26–49. https://doi.org/10.1111/j.1468-2427.2005.00568.x

Gangadharan, S. P. (2017). *The downside of digital inclusion: Expectations and experiences of privacy and surveillance among marginal Internet users.* https://journals.sagepub.com/doi/abs/10.1177/1461444815614053

Ghana Ministry of Finance. (2020). *Digital Financial Services Policy*. https://mofep.gov.gh/publications/acts-and-policies/strategic-documents-on-financial-sector

Gillwald, A. (2020, March 10). *Data, AI & Society*. https://researchictafrica.net/2020/03/10/data-ai-society/

Gillwald, A., & Mothob, O. (2019). *A Demand-Side View Of Mobile Internet From 10 African Countries* (After Access Policy Paper No. 7, Series 5; Policy Paper Series 5: After Access-Assessing Digital Inequality in Africa). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Gillwald, A., & Mothobi, O. (2019). *After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries* (After Access 2018: A Demand-Side View of Mobile Internet from 10 African Countries After Access: Paper No. 7 (2018); Policy Paper Series No. 5). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf

Gillwald, A., Mothobi, O., & Rademan, B. (2018). *The State of ICT in South Africa* (After Access Policy Paper No. 5, Series 5; Policy Paper Series 5: After Access-Assessing Digital Inequality in Africa). Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

Question to the Minister of Home Affairs—NW1176 | PMG, Parliamentary Question (2020) (testimony of Member of Parliament Gondwe). https://pmg.org.za/committee-question/14098/

Government of South Africa. (n.d.). *Smart Identity Document (ID) card roll-out | South African Government*. South African Government. Retrieved 21 April 2021, from https://www.gov.za/about-government/government-programmes/smart-identity-document-id-card-roll-out

Greenleaf, G. (2011). Independence of Data Privacy Authorities: International Standards and Asia-Pacific Experience. *Computer Law & Security Review*, *18*(1 & 2). https://ssrn.com/abstract=1971627 or http://dx.doi.org/10.2139/ssrn.1971627

GSMA. (2019). *Digital identity opportunities for women: Insights from Nigeria, Bangladesh, and Rwanda*. https://www.gsma.com/mobilefordevelopment/blog/digital-identity-opportunities-for-women-insights-from-nigeria-bangladesh-and-rwanda/

Gurumurthy, A., & Chami, N. (2019). *The Wicked Problem of AI Governance*. https://doi.org/10.13140/RG.2.2.14753.22886

Hao, K. (n.d.). *AI is sending people to jail—And getting it wrong*. MIT Technology Review. Retrieved 12 February 2019, from https://www.technologyreview.com/s/612775/algorithms-criminal-justice-ai/

Hastings-Spaine, N. (2021, January 5). *How BACE Group is Building Facial Recognition Tech for Africa*. Built in Africa. https://www.builtinafrica.io/blog-post/charlette-nguessan-bace-group

Hong Chang, M., & Kuen, H. C. (2019). Towards a Digital Government: Reflections on Automated Decision-Making and the Principles of Administrative Justice. *Singapore Academy of Law Journal*, *31*(2), 875–906.

Hunter, M. (2020). *Track and trace, trial and error: Assessing South Africa's approaches to privacy in Covid-19 digital contact tracing* (The Media Policy and Democracy Project). Department of Communication Science at the University of South Africa; Department of Journalism, Film and Television at the University of Johannesburg. https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/track-and-trace-digital_contact-tracing-in-sa-nov-2020.pdf

Izaguirre, J. C., Kaffenberger, M., & Mazer, R. (2018, September 25). *It's Time to Slow Digital Credit's Growth in East Africa*. https://www.cgap.org/blog/its-time-slow-digital-credits-growth-east-africa

Jain, R., Bassier, I., Budlender, J., & Zizzamia, R. (2020). *The labour market and poverty impacts of COVID-19 in South Africa: An update with NIDS-CRAM Wave 2* (Wave 2). National Income Dynamics Study.

Klaaren, J. (2021a). The ermergence of regulatory capitalism in Africa. *Economy and Society*, *50*(1), 100–119.

Klaaren, J. (2021b, February 26). *South Africa's Technologies Enhancing Contact Tracing for COVID-19: A Comparative and Human Rights Assessment*. The COVID-19 Pandemic, Inequalities and Human Rights In South Africa, Online: Zoom.

Kolawole, O. (2020, September 23). How Ghanaian-based biometric startup, BACE Group is tackling identity theft in Africa. *Techpoint Africa*. https://techpoint.africa/2020/09/23/bace-group-biometric-startup/

Leibbrandt, M., Woolard, I., McEwan, H., & Koep, C. (2015). *Employment and inequality outcomes in South Africa*. ResearchGate. https://www.researchgate.net/publication/266214017_Employment_and_inequality_outcomes_in_South_Africa

Mahlaka, R. (2021, January 25). *ANC policymakers endorse a basic income grant, but it is still far from being implemented*. Daily Maverick. https://www.dailymaverick.co.za/article/2021-01-25-anc-policymakers-endorse-a-basic-income-grant-but-it-is-still-far-from-being-implemented/

Malinga, S. (2020a, August 5). *GovChat gets global recognition with UNICEF partnership*. ITWeb. https://www.itweb.co.za/content/DZQ58MVPAyJvzXy2

Malinga, S. (2020b, September 4). *GovChat saves SASSA R7.5m through chatbot service*. ITWeb. https://www.itweb.co.za/content/dgp45va63Pn7X9l8

Margele, B., & Ngubane, N. (2018, August 30). Net1 Accused of Duping Social Grant Beneficiaries. *Fin24*. https://www.fin24.com/Companies/ICT/net1-accused-of-duping-social-grant-beneficiaries-20180830

Marwala, T. (2015). *Impact of Artificial Intelligence on Economic Theory*. https://www.researchgate.net/publication/281486806_Impact_of_Artificial_Intelligence_on_Economic_Theory

Masango, M. of P. (2020, June 17). *Question NW974 to the Minister of Social Development*. Parliamentary Questions (National Assembly). https://pmg.org.za/committee-question/13806/

Matthers, A. (2019, April 5). How Artificial intelligence can usher a new wave of Identity Verification services? *MarkTechPost*. https://www.marktechpost.com/2019/04/05/how-artificial-intelligence-can-usher-a-new-wave-of-identity-verification-services/

McLeod, D. (2021, March 25). *Facebook interdicted in fight with South Africa's GovChat—TechCentral*. Tech Central. https://techcentral.co.za/facebook-interdicted-in-fight-with-south-africas-govchat/106003/

McQuoid-Mason, D. (2014). Privacy. In *Constitutional Law of South Africa: Commentary* (2nd ed.). Juta.

Mhlambi, S. (2020). *From Rationality to Relationality: Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance* (Carr Center Discussion Paper). Harvard Kennedy School.

https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial

MyBroadband. (2020, February 12). *19 new bank branches where you can get your South African smart ID and passport in 2020* [Business Tech]. https://businesstech.co.za/news/banking/373192/19-new-bank-branches-where-you-can-get-your-south-african-smart-id-and-passport-in-2020/

Mzekandaba, S. (2019, May 31). *R20m funding injection for GovChat*. ITWeb. https://www.itweb.co.za/content/LPp6V7r4wlOqDKQz

Mzekandaba, S. (2020, September 29). *GovChat ready to 'assist SASSA where needed'*. ITWeb. https://www.itweb.co.za/content/mYZRXv9aEJavOgA8

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1). *THRHR*, *79*, 51.

Nortier, C. (2020, October 13). *MAVERICK CITIZEN: COVID Alert SA app: The fine balance between public health, privacy and the power of the people*. Daily Maverick. https://www.dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/

Osabuohien, E., & Karakara, A. (2018). ICT Usage, Mobile Money and Financial Access of Women in Ghana. *Africagrowth Agenda Journal*, *15*(1). https://www.researchgate.net/publication/327201794_ICT_Usage_Mobile_Money_and_Financial_Access_of_Women_in_Ghana

Ostrom, E., & Ostrom, V. (1977). Public Goods and Public Choices. In *Alternatives for Delivering Public Services: Towards Improved Performance*. Westview Press.

Owusu-Oware, E. K., Effah, J., & Boateng, R. (2017). *Institutional Enablers and Constraints of National Biometric Identification Implementation in Developing Countries: The Case of Ghana*. Twenty-third Americas Conference on Information Systems, Boston, MA. https://aisel.aisnet.org/amcis2017/ICTs/Presentations/13/

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press; JSTOR. https://www.jstor.org/stable/j.ctt13x0hch

Pather, R. (2017, March 15). CPS director Serge Belamant: We work for profit. *Mail & Guardian*. https://mg.co.za/article/2017-03-15-cps-director-serge-belamant-we-work-for-profit/

Payne, S. (2021, January 22). *Eyebrows raised over amount of Western Cape Sassa disab...* Daily Maverick. https://www.dailymaverick.co.za/article/2021-01-22-eyebrows-raised-over-amount-of-western-cape-sassa-disability-applications-as-water-cannon-inquiries-continue/

Plantinga, P., Adams, R., & Parker, S. (2019). Global Information Society Watch 2019: AI technologies for responsive local government in South Africa. In A. Finlay (Ed.), *Artificial Intelligence: Human rights, social justice and development* (pp. 215–220). Association for Progessive Communications. http://repository.hsrc.ac.za/handle/20.500.11910/15173

PricewaterhouseCoopers. (2018). *PwC's Global Artificial Intelligence Study: Sizing the prize*. https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Privacy International. (2013). *Biometrics: Friend or foe of privacy?* [Briefing]. https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy

Privacy International. (2019, January 31). *Understanding Identity Systems Part 3: The Risks of ID*. Privacy International. http://privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id

Qorbani, R. (2017). *How Machine Learning Truly Applies To Digital Identity*. https://www.forbes.com/sites/forbestechcouncil/2017/11/27/how-machine-learning-truly-applies-to-digital-identity/#1d4de3577f2b

Question NW973 to the Minister of Social Development, (2020) (testimony of B Masango). https://pmg.org.za/committee-question/13831

Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2020). Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 145–151. https://doi.org/10.1145/3375627.3375820

Razzano, G. (2020a). Good ID and Financial Inclusion: A call for context. *Research ICT Africa*. https://researchictafrica.net/2020/02/05/good-id-and-financial-inclusion-a-call-for-context/

Razzano, G. (2020b, February 5). *Good ID and Financial Inclusion: A call for context*. https://researchictafrica.net/2020/02/05/good-id-and-financial-inclusion-a-call-for-context/

Razzano, G. (2020c). *The public-private: A key legal nexus for South Africa's AI future* (Policy Brief No. 6). Research ICT Africa. https://researchictafrica.net/publication/the-public-private-a-key-legal-nexus-for-south-africas-ai-future/

Razzano, G. (2020d, November 5). *Digital Hegemonies for COVID-19* [Global Data Justice]. https://globaldatajustice.org/covid-19/digital-hegemonies-south-africa

Razzano, G. (2021). *Understanding the Theory of Collective Rights: Redefining the Privacy Paradox* [Concept Note]. Research ICT Africa. https://researchictafrica.net/publication/concept-note-understanding-the-theory-of-collective-rights-redefining-the-privacy-paradox/

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Matanga, C., Rens, A., & van der Spuy, A. (2020). *SADC Parliamentary Forum Discussion Paper: The Digital Economy and Society*. Research ICT Africa. https://researchictafrica.net/publication/sadc-pf-discussion-paper-the-digital-economy-and-society/

Razzano, G., Spuy, A. van der, & Rens, A. (2020, June 24). Waiting for POPIA. *Research ICT Africa*. https://researchictafrica.net/2020/06/24/waiting-for-popia/

Reed, C., & Ng, I. (2019). *Data Trusts as an AI Governance Mechanism* (SSRN Scholarly Paper ID 3334527). Social Science Research Network. https://doi.org/10.2139/ssrn.3334527

Royal Academy of Engineering. (2020, September 3). *First woman to win the Africa Prize for Engineering Innovation—Royal Academy of Engineering*. https://www.raeng.org.uk/news/news-releases/2020/september/first-woman-to-win-the-africa-prize

Salaudeen, A. (2020, September 7). *A 26-year-old is first woman to win the Royal Academy of Engineering's Africa Prize*. CNN. https://www.cnn.com/2020/09/07/africa/africa-engineering-prize-intl/index.html

Sandhu, K., & Balakumaran, R. (2017). *Function Creep and Fintech in India: The Aadhar ID System.* (Part 1; Trading Faces).

Sen, A. (2005). Human Rights and Capabilities. *Journal of Human Development*, *6*(2), 151–166. Academic Search Premier.

Shapshak, T. (2018, September 10). *Renowned African Incubator MEST Celebrates 10 Years With $700,000 Investment*. Forbes. https://www.forbes.com/sites/tobyshapshak/2018/09/10/renowned-african-incubator-mest-celebrates-10-years-with-700000-investment/

Singh, K. (2021, January 8). *Home Affairs proposes new identity policy*. IOL News. https://www.iol.co.za/mercury/news/home-affairs-proposes-new-identity-policy-a7fc4211-fed0-4162-adf0-13f42d97c5e9

Srinivasan, J., Bailur, S., Schoemaker, E., & Seshagiri, S. (2018). Privacy at the margins| The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication*, *12*, 20.

Srinivasan, J., & Oreglia, E. (2020). The Myths and Moral Economies of Digital ID and Mobile Money in India and Myanmar. *Engaging Science, Technology, and Society*, *6*(0), 215–236. https://doi.org/10.17351/ests2020.276

Staff Writer. (2020, September 18). *South Africa harnesses artificial intelligence, machine learning in Covid-19 fight*. IOL News. https://www.iol.co.za/business-report/companies/south-africa-harnesses-artificial-intelligence-machine-learning-in-covid-19-fight-9f9b0dba-65d4-41a8-8196-cd2258fae312

Staff Writer. (2021, January 27). South Africa wants a new ID system – but Home Affairs needs to fix long queues and IT failures first. *BusinessTech*. https://businesstech.co.za/news/it-services/463728/south-africa-wants-a-new-id-system-but-home-affairs-needs-to-fix-long-queues-and-it-failures-first/

Stahl, B. C. (2021). *Artificial Intelligence for a Better Future An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies*. Springer Publishing.

Statistics South Africa. (2018). *General Household Survey, 2018*. Statistics South Africa. http://www.statssa.gov.za/?s=general+household+survey&sitem=publicatio

Suchman, L., Follis, K., & Weber, J. (2017). *Tracking and Targeting: Sociotechnologies of (In)security*. https://journals.sagepub.com/doi/abs/10.1177/0162243917731524

Szigeti, H., Messadi, M., Majumdar, A., & Eynard, B. (2011, October). STEEP analysis as a tool for building technology roadmaps. *ResearchGate*. eChallenges e-2011, Florence, Italy. https://www.researchgate.net/publication/301295850_STEEP_analysis_as_a_tool_for_building_technology_roadmaps

Thiel, A. (2020). Biometric identification technologies and the Ghanaian 'data revolution'. *The Journal of Modern African Studies*, *58*(1), 115–136. https://doi.org/10.1017/S0022278X19000600

Thorat, S. B., Nayak, S. K., & Dandale, J. P. (2010). Facial Recognition Technology: An analysis with scope in India. *ArXiv*.

Vally, N. (2016). *Insecurity in South African Social Security: An Examination of Social Grant Deductions, Cancellations, and Waiting*. ResearchGate. https://www.researchgate.net/publication/308955644_Insecurity_in_South_African_Social_Security_An_Examination_of_Social_Grant_Deductions_Cancellations_and_Waiting

Wachter, S., & Mittelstadt, B. (2018). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review*.

Wagner, K. (2020, December 10). *Facebook (FB) Plans to Turn Messaging App WhatsApp Into a Moneymaking Business*. Bloomberg. https://www.bloomberg.com/news/features/2020-12-09/facebook-fb-plans-to-turn-messaging-app-whatsapp-into-a-moneymaking-business

Western Cape Government. (2021, March 2). *Applying for an Identity Document*. Western Cape Government. https://www.westerncape.gov.za/service/applying-identity-document

Wilson SC, J., & Berger, J. (2021). *GovChat Proprietery Ltd and Another \\ Facebook Inc. And Another: Respondent's Heads of Argument*.

Wirtz, B. W., & Weyerer, J. C. (2019). Artificial Intelligence in the Public Sector. In A. Farazmand (Ed.), *Global Encyclopedia of Public Administration, Public Policy, and Governance* (pp. 1–7). Springer International Publishing. https://doi.org/10.1007/978-3-319-31816-5_3701-1

World Bank. (2018, September 20). *Ghana Receives Support to Strengthen its Financial Sector and Promote Inclusion* [Text/HTML]. World Bank. https://www.worldbank.org/en/news/press-release/2018/09/20/ghana-receives-support-to-strengthen-its-financial-sector-and-promote-inclusion

World Bank. (2019). *Identification for Development (ID4D) 2019 Annual Report (English)*. World Bank Group. http://documents.worldbank.org/curated/en/566431581578116247/Identification-for-Development-ID4D-2019-Annual-Report

Yin, R. (2018). *Case Study Research and Applications: Design & Methods* (6th ed.). Sage Publications.

Zuboff, S. (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Penguin Publishing Group. https://antipodeonline.org/wp-content/uploads/2019/10/Book-review_Whitehead-on-Zuboff.pdf