MY DATA RIGHTS
Feminist Reading of the Right to Privacy and Data Protection in the age of AI

By Chenai Chair
Acknowledgements:

This research was made possible with funding support from Mozilla. Thank you to everyone who participated in this project in various ways. Thank you to the team that helped in the final report production.

Review by - Amanda Manyame, Janice Wait and Joy Banda

Report design - Lisa Chivanga

Editor - Rumbidzai Matamba

Report communications oversight - Sabine Matsheka
# Table of Contents

- Executive Summary ............................................. 1
- Introduction ......................................................... 4
- Understanding why gender matters ..................... 4
- AI Discourse in South Africa ............................... 6
- Uneasy Access - Gendered concerns .................. 8
- Perceived concerns of data harms ....................... 10
- Privacy and data protection – assessing adequacy of the law ................................. 13
- Gendered analysis of data protection - is it sufficient? ........................................... 15
- Conclusion ......................................................... 18
- Recommendations ................................................ 18
- Annexures ............................................................ 20
- Bibliography ......................................................... 22
Executive Summary

The triple threat of high inequality, poverty and unemployment, remnants of colonisation and apartheid adversely affects women, gender diverse people and sexual minorities more at various intersections including race and class. The crisis of gender-based violence disproportionately affects women, girls, and non-gender conforming individuals such as lesbian, gay, bisexual, transgender and/or intersex people. The existent injustices that marginalised groups and sexual minorities face shape how they experience technology, policy, and regulation – either to achieve social justice or increase current inequalities and harms.

In the era of AI based innovations such as automated decision making and algorithms this context is important to understand how we can safeguard against harms and injustices while using these technologies to dismantle barriers of oppression. The development, implementation and governance of AI based innovations, especially around data that is fed into them, raises important questions on their impact on society and digital rights.

This research seeks to respond to the following questions:

1) What would a gender-responsive data protection and privacy law entail to ensure gender safeguards against AI gendered harms?

2) How can civil society play a role in ensuring a gender transformative law and practice with a focus on the right to privacy and data protection?

The feminist conceptual lens draws from data feminism, intersectionality, data justice and feminist principles of the internet. The conceptual lens allows one to ask questions of who is being represented and by whom; whose interests are being centered; why this discussion is important and how it is taking place, which allows for criticism of power and how data itself can be used to ensure justice in society.

The methodological approach for this paper includes qualitative interviews to understand the current AI ecosystem and related privacy and data protection laws in South Africa. A targeted quantitative survey with open ended questions was shared with selected activists that work on gender and sexual justice issues to gauge perceptions of concerns with privacy and data protection. Recommendations on how civil society may intervene were drawn from there. The necessary ethical protocols were followed based on feminist internet ethical research practices.

This paper identifies the following key takeaways:

AI Discourse in South Africa

AI innovative solutions are on the rise in South Africa largely being driven by the private sector's need for a competitive edge in markets and the public sector's need for efficient developmental solutions. Policy conversations on governing AI have begun in the country with a focus on ensuring economic gains through the creation of employment opportunities by upskilling citizens; being innovative enough to attract global business as well as legal and regulatory compliance for global trade. The Presidentially appointed Fourth Industrial Revolution Commission has recommended the establishment of an Artificial intelligence institution. However, concerns have been raised that there is a risk of perpetuating digital disparities and inequality in the discourse around AI.
Uneasy Access - Gendered concerns of AI

The right to privacy from a gender perspective is particularly important as access to digital platforms may be problematic for women and gender diverse people with continuation of existing patriarchal dynamics online from offline realities. Issues emerging from a gender perspective include the lack of agency and control over data, problematising consent in contexts of unequal power dynamic, loss of privacy, discrimination, and bias at the intersection of race, class, and gender.

Perceived concerns of AI harms

The research conducted finds that there is in general a lack of documentation on harms in the South African context. For the purposes of this paper, five AI scenarios were therefore given to survey participants for them to reflect on how these harms would play out in the South African context and in relation to their areas of work. Key contextual issues that were recurring references were race, economic status, homophobia, and gender-based violence. The issues around bias, discrimination and increased surveillance were raised as likely to be of concern.

Responsiveness of current Protection of Personal Information Act to AI and gender issues

The country’s Protection of Personal Information Act (2013) is the focus of assessment as it is an existing regulatory framework that has relevance to both the current governance of data and AI, as well as the conceptualisation and interpretation of new policies in this space. As the law was set up close to two decades ago there are significant gaps with AI specific provisions although there is a safeguard for automated decision making. The analysis found a need for the current law to be contextually responsive, address the issue of gender exclusionary language (he/she used in the text) and the lack of nuance of gender and sexuality harms embedded into the law. There were examples of civil society making use of the law to challenge surveillance issues however a gendered nuance is missing.

To be gender responsive means to design and implement policies that consider gendered realities of the society we live in and ensure that injustices are not replicated as we race towards digital development. The following recommendations are put forward on how this can be done with diverse stakeholders.

The recommendations stemming from this paper cover four important areas.

1) Policy and regulation:

Policy and regulation would require context-based implementation and assessment of current and future privacy and data protection laws with regards to Artificial Intelligence innovations. This would be complemented by collaboration between Civil Society, the legal community, and other relevant stakeholders.

2) Research and documentation:

Research and documentation are necessary to fill the knowledge gap in understanding the context-based impact of AI based innovations. Case studies documenting the impact of AI on marginalised groups would highlight the necessary responsive means to safeguarding against harms and injustices. Research may also be used to support development of governance models and develop AI registrars to document the proliferation of AI, where it is used and the impact it has. Resourcing these initiatives to ensure their public and open resources is important.

3) Public awareness:

Public awareness requires collaborative,
relatable, and innovative campaigns to raise understanding of the opportunities and challenges of AI with regards to privacy and data protection. Public awareness would focus on campaigns for diverse marginalised groups, creation of collaborative spaces that are safe for gender and sexual minorities to learn and raise their concerns and resourcing from different stakeholders to ensure the necessary support needed for public participation.

4) Responsibility of technical community:

The technical community carries the responsibility of carrying out public engagement and sharing information on how their systems work to ensure accountability and trust of AI based innovations. Civil society can be drawn into ethical guideline development that is cognisant of experiences of injustice for marginalised groups. In design and implementation of AI based solutions – digital literacy, privacy by design and context responsiveness should form underlying guiding principles in designing solutions that would not lead to further social injustices.
INTRODUCTION

Artificial intelligence (AI) and machine learning based solutions are part of the focus of technological development in the context of the Fourth Industrial Revolution in South Africa. These technologies are part of our daily use - social media platforms rely on algorithms for content moderation and financial services use automated decision-making systems to increase efficiency. However, the development, implementation and governance of these AI based innovations, especially around data that is fed into them, raises important questions on their impact on society and digital rights. Of concern is how personal information feeds into the development of AI based innovations and, regardless of it being in the form of de-identified aggregate data, shapes the way in which people experience privacy from a gender

Focusing on gender inequalities demands a gender centred approach to interrogating new technologies that are being implemented, from conceptualisation and design, to the safeguards that have been put in place to ensure that inequalities are not exacerbated.

As the focus on AI ramps up, the question of whether South Africa is ready to harness the opportunities it presents while, at the same time, ensuring safeguards for human rights and, by extension, digital rights becomes critical. This research focuses on the impact of new technology and adequacy of policy and regulation by centering the realities of women and gender diverse people in South Africa through a feminist lens.

This paper responds to the following research questions:

1) What would a gender-responsive data protection and privacy law entail to ensure gender safeguards against AI gendered harms?

2) How can civil society play a role in ensuring a gender transformative law and practice with a focus on the right to privacy and data protection?

A feminist conceptual framework drawing from data feminism principles, intersectionality, data justice and feminist principles of the internet has been used in the design and review of this project. Qualitative in depth interviews and a targeted quantitative survey has been carried out with identified digital rights, gender and sexual justice activists, technical, community and policy analysts, and legal experts. The purpose has been to gauge awareness and concerns regarding privacy and data protection with the uptake of AI-based innovations, from a gendered perspective. Recommendations for policy makers and civil society are provided as ways for ensuring gender responsive policies and implementation.

Understanding why gender matters

The young democracy of South Africa, continuously leads in economic development, ranked as the second biggest economy on the continent. \(^1\) South Africa is also one of the leaders in internet use with over half of the population (53%) having access to the internet. \(^2\) Connectivity is well developed in urban and semi-urban areas with gaps remaining in rural areas. Digital inequalities between men and women in South Africa are reflective of underlying inequalities in education and income between men and women which impacts access and use of the internet. \(^3\)
The triple threat of high inequality, poverty and unemployment, remnants of colonisation and apartheid impacts the social fabric of South Africa. South Africa’s inequality is steeped in layers of race, spatial distribution and gender which impacts how its society experiences this triple threat. Although women represent approximately half of the population in the country, there remains inequality with gender gaps in income and labour market, with limited labour market participation in contrast to men. The gender wage gap is stark with women’s monthly earnings remaining around 70% of men’s earnings.

In addition to this economic inequality, the crisis of gender-based violence disproportionately affects women, girls and non-gender conforming individuals such as lesbian, gay, bisexual, transgender and/or intersex people. Gender based violence in South Africa manifests itself as intimate partner violence and/or sexual violence and is usually perpetrated by men. In the current health pandemic, together with having the highest recorded cases of COVID-19 infections on the continent, gender-based violence cases spiked as lockdown measures were instituted.

To understand the context of violence in South Africa, Pumla Dineo Gqola in ‘Rape A South African Nightmare’ highlights the complexity and societal attitudes towards which we may see rape as a norm and excuse it and, at the same time, the toxic masculinity discourse.

The inequalities in the experience of marginalised groups and sexual minorities result in different experiences with technology, policy, and regulation. In the era of AI based innovations such as automated decision making and algorithms this context is important to understand how we can ensure data justice. After all, the reproduction of power asymmetries shows that the rationality of computers or of humans programming the machines does not always take context into account.

3 Gillwald (n 30).
**AI Discourse in South Africa**

AI is a wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence. However, there is often concern about what truly makes something an AI. For the purpose of this paper, we draw on Mozilla’s understanding of AI including algorithms and automated systems, machine learning systems and the actors involved in the process.  

AI is seen through a developmental and economic growth paradigm in the context of emerging markets. Abeba Birhane describes the discourse of AI-based innovations in some circles being taken up with much enthusiasm as follows:

> Mentions of ‘technology’, ‘innovation’ and AI continually and consistently bring with them evangelical advocacy, blind trust and little, if any, critical engagement. They also bring with them invested parties that seek to monetize, quantify and capitalise every aspect of human life often at any cost.  

AI discourse often focuses on (i) its capabilities - the growth of economies, increase in production, reduction in labour costs etc. and (ii) the regulation of data processors and data controllers and the ways in which people’s data can be protected in order to give effect to the rights of privacy and access to information, which are protected by most African constitutional decrees. In South Africa, AI based innovations and solutions are being deployed in various service industries including the financial sector, transport and logistics, agriculture, facial recognition systems, public sector and by civil society. This research found that they are mainly driven by the private sector with solutions for making business more efficient and the public sector with a focus on smart cities. Unsurprisingly so as a participant in the research pointed out, the AI development sector is more responsive to business needs than societal issues. A few examples were found of AI based innovations responsive to society – such as Soul City’s and AI for Good’s rAlnbow – an AI based chatbot over Facebook messenger designed to support gender-based violence victims and survivors. Public interest technical communities have also been developing AI based innovations such as Masakhane - a grassroots Natural Language Processing community focused on African Languages and Deep Learning IndabaX a South African AI and machine learning community.  

Despite of this progress, men dominate this field and the over-representation of men in the design of AI and technologies could quietly undo decades of advances in gender equality. The 2018 AI Index reported that women are severely underrepresented in university faculties and, consequently, as candidates for jobs in the AI sector. On the continent, women account for only 28% of science researchers while men dominate at 72%. There is a call for more women’s representation in leadership and participation within the science.

---

5 Statistics SA (n 22).
6 Statistics SA (n 22).
8 Safer Spaces (n 26).
technology, engineering, and mathematics (STEM) field in South Africa. The lack of representation plays out in the lack of critical engagement on the stereotypes that may be reinforced by some AI based innovations. For example, the way in which AI is gendered often frames women in subservient positions such as the use of female names in voice recognition systems and the use of “female personas” as digital assistants. As one interview respondent pointed out, specific to these examples of female personas, oftentimes the gender stereotype effect would not have been thought of in design and implementation of the system. In the South African context there is a need to assess if and how race, sexuality and class stereotypes may be reflected in AI based innovations.

While there is no specific AI policy, policy conversations on AI based innovations also focus on ensuring economic gains through the creation of employment opportunities by upskilling citizens; being innovative enough to attract global business; as well as legal and regulatory compliance for global trade. South Africa's policy focus is on AI and data diversity in different sectors and building the necessary capacity for global engagement. More specifically, the dream for South Africa is “a globally competitive, inclusive and shared economy with the technological capability and production capacity that is driven by people harnessing the 4IR to propel the country forward towards its social and economic goals, instead of falling behind.”

In its 2019 White Paper, the Department of Science and Information (DSI) focused on how emerging technologies may be used for inclusive economic growth by capturing policy commitments to address poverty, inequality and unemployment. The 2020 National Planning Commission report on ‘Digital Futures’ assessing South Africa’s readiness for the Fourth Industrial Revolution provides insight on the readiness and the necessary policy interventions required to use these technologies for development. The 4IR Commission, set up by the President of South Africa to provide leadership for society to understand, navigate and assume agency of a technologically evolving future, leads the way in guiding the take up of technology and developing policies prioritised on inclusive economic growth. The commission recommends the establishment of an Artificial intelligence Institution. The commission’s recommendations on policy focus on building the capacity of policy makers to become 4IR and science literate so as to make policy decisions that are holistic, that are responsive to the logics of the technologies, the industries they will have an impact on, the people who will both consume and produce them, and the policy and legislative agility required to compete on a global stage.

While the current moves are exciting in response to AI, critics point out the current risk of perpetuating digital disparities and inequality in the discourse around AI. Given the existent varying levels of gendered inequality, women and gender diverse people may be the last to capture the benefits of the Fourth Industrial Revolution. Therefore, the replication of existing inequalities, new social injustices and unequal power dynamics will impact the differences in experiences of these new technologies.

Uneasy Access - Gendered Concerns

The right to privacy from a gender perspective is particularly important as “with gender stereotypes comes problems of privacy invasion and abrogation”. 33 Anita Allen frames this as ‘un-easy access’ which helps in highlighting the way in which access to the internet may be problematic for women and gender diverse people as the continuation of existing power dynamics and control from offline realities. 34 Power dynamics and control over data are seen in the disregard for agency as the work by Privacy International highlights how period tracking applications collected and used intimate data and personal information for their monetary gain via third party exchanges without informing their users. 35

As the feminist principles of the internet highlight, agency is important to establish an internet that would transform gendered inequalities in society. The feminist principle of privacy and data focuses on the ability to have control over your information and to understand how it is being used, reject the ‘for profit only’ focus on data use and manipulative behaviour such as targeted advertisements. Most narratives around data focus on it as if it were an entity that exists outside our personhood, however, data is a part of us and our experiences of data and privacy embody the concept of ‘data bodies’. 36

Consent is often key when thinking of data and data protection for the rights of people, but when located in the current context, the question becomes - do people have the power, ability, and capacity to say no? 37 A South African example in the ability to meaningfully consent for vulnerable groups is raised in access to social services grants. As an interview respondent pointed out one is not a position to negotiate their data being collected or not when that data determines access to social safety nets. This public data has also raised concerns of the need to protect to respect individuals’ rights to privacy and ensure safeguards against state surveillance. 38 For example, there has been unauthourised use of data to exploit social grant recipients’ data after an unlawful contract between the South African Social Services Agency (Sassa) and Cash Paymaster Services (CPS). 39

Loss of privacy, discrimination by gender or health, data breaches, and harms due to machine or algorithm bias form some of the injustices in societies driven by data. 40 Table 1 provides examples of some of the related harms that this project has mapped over the course of the year drawn from European and North American research. The significant challenge in this study has been the lack of local examples of gendered harms and a future area of work. One specific case that was referred to was gendered and racial discrimination in the South African banking sector impacting access to finance. 41

As was indicated by our research participants, the issue of racial and gendered bias in the banking sector is within the context of problematic existent data that although race and gender data is not used per se in the decision making other data that is used to determine loans highly affects groups that were financially marginalised based on historical legacies of apartheid – mainly gender and racial perspective. 42

Discrimination | Social Bias | AI relying on algorithms learnt from real-world data can, inadvertently, reinforce existing social biases.

Discrimination | Gender, weight, skin tone | The body imaging technologies that are now used in many airports around the world to screen passengers are often represented as objective and neutral, yet the aim of using such technologies is to police non-normative bodies which means that some bodies are more likely to be treated as a potential threat.

Publication and sharing of non-consensual explicit material | Gender | AI-generated fake videos (deepfakes) are becoming more common and, as with everything, women are being disproportionately affected by them as seen through deepfake porn.

Harassment | Malice, gender, gender identity | The use of targeted anti-LGBTQI+ ads on LGBTQI+ online platforms is malicious and psychologically harmful.

Stereotyping | Automated discrimination | The use of gendered ‘voices’ and ‘responses’, in addition to the use of gendered pronouns and syntax, tend to perpetuate harmful gender stereotypes.

Racism | Racial bias | AI technologies have also been guilty of racism - from misidentifying some of the most iconic black women in the present day such as Michelle Obama, Serena Williams and Oprah Winfrey, to labelling black people in images as gorillas, which is a racist trope.

Economic harm | Gender bias | There is evidence of targeted ads where algorithms are perpetuating the pay gap by targeting listings for better-paid jobs towards men.

Surveillance | Unauthorised surveillance | Contrary to international human rights law, governments are engaging more and more in mass surveillance, mostly merely because they can.

Ethnicity and race | | A range of interacting characteristics – race, ethnicity, religion, gender, location, nationality, socio-economic status – determine how individuals become administrative and legal subjects through their data and, consequently, how this data can be used to act upon them by policymakers or commercial firms. The possibility of being identified as a target of surveillance multiplies depending on the number of categories of interest one belongs to.

Table 1: Gender based harms related to Artificial Intelligence based systems

Perceived concerns of data harms

To counter the lack of documentation on harms in the South African context, AI scenarios were given to survey participants for them to reflect on how these harms would play out in the South African context and in relation to their areas of work. In assessing awareness of privacy and data protection in general, 95% of the participants knew data, in the form of personal information, was being generated because of being connected digitally. The collection and processing of this data is of great concern in terms of who has access to this information (95%); the way in which this information will be used (90%) and where the information would be stored and processed (86%). As one survey participant shared:

“Harassment and the usage of our data [is a concern]. Privacy is of most importance in the work we do because we deal with people who are seeking terminations of pregnancy in a society with stigma. They want their information to be private and we use social media to do our work.”

The current laws do provide provisions on data subjects’ rights to be informed about the collection, processing and use of their personal data. The limitation with AI, however, is that the data sets are built up of overall collected data – it is this aggregate data with an impact on communities and individuals beyond personal information. It also takes away from consent as the data forms part of data sets that it was not initially processed for.

The second scenario focuses on the monitoring of online activities and how they may build user profiles for purposes of targeted advertising, for example. Personal information that may otherwise be publicly available which can be found on social media networks and data not generally sensitive, may actually generate sensitive data that may be harmful in particular contexts. The categorisation of data into sensitive and non-sensitive data is a recurring feature in most pieces of data protection legislation and yet, through processes such as profiling, detailed and highly comprehensive profiles can be developed from what is seemingly unimportant or “non-sensitive” data. Profiles are used to make automated and consequential decisions such as hiring, credit scoring or national security. Therefore, as much as there is data regulation that allows you to object to the use of your data or the right to know how your data is being used, it is unable to account for issues emerging with AI.

In this instance all participants were aware of this activity and privacy and data protection was a great concern. Concerns that emerged were related to the type of information they worked with – sensitive information or planned activities. In addition, activists were greatly concerned with how their location data seems easily available influencing targeted advertising across platforms, yet this could mean they could also be targets for those against their work.

In addition, the type of content that comes their way as the result of the profile they fit into was of concern. One respondent pointed out that because of working on gender identities and sexualities, the adverts or spam email they received was often in the form of harassment and/or violent. The adverts also perpetuate harmful stereotypes and prejudices. One of the most interesting insights was related to the access of reproductive rights – when women search for abortion services it was pointed out that they seem to be directed to illegal abortion service providers – which infringes on access to safe abortions. The POPIA, in section 69, focuses on the prohibition of targeted direct marketing by means of unsolicited electronic communication, but profiling for targeted advertising is not covered. 45

The third scenario focused on discrimination because of profiles built of users even from online behaviour. The example used focused on the way in which algorithms perpetuate the gender pay gap by showing better paying jobs to men and employed the example of Amazon’s hiring tool that was biased against women. Half of the respondents were aware that this was an issue. The majority, 18 respondents to be precise, were concerned about privacy and data protection in this context. As this was an example based in a different context, 90% of the respondents indicated this as important in the case of South Africa.

Race, ethnicity, location, citizenship, health status, digital connectivity, and gender were raised as potential points of discrimination in South Africa, although this is protected against at individual level by the Constitution, Labour Relations Act 1995, The Promotion of Equality and Prevention of Unfair Discrimination Act, 2000, and in the POPIA. However, discrimination using automated decision-making systems happens when one fits a flagged profile that is indicative of race and gender through the aggregated data. Racial and gender discrimination in accessing financial services was raised by five of the respondents as a major concern related to AI:

“It has been reported that this is a problem in the banking sector where AI is racist and sexist. Black women will thus stand no chance when applying for loans. I would be surprised if one’s geographical location does not automatically exclude many from opportunities. Of concern are people from the rural areas, townships, informal settlements, and crime infested areas.” 46

The fourth scenario focused on surveillance by drawing on the roll out of CCTV or surveillance cameras and facial recognition systems in South Africa. There was a high level of awareness of this roll out and 73% of the participants found this to be a relevant issue of privacy and data. Two issues were highlighted as the most significant for participants – 81% of the participants were concerned about how the technology may be used to invade their privacy and, at the same time, 64% saw the usefulness of surveillance cameras to address crime. This issue was
highlighted as a need to balance security and privacy. In thinking about other issues that may be relevant in the South African context, bias, discrimination and misuse of data for purposes of profiling were raised as concerns of the surveillance emerging from these technologies. This was a concern in a country where police brutality is rife – this technology could be used for further discrimination and violence towards individuals. Race was a big underlying concern as these technologies may be used to profile black people in areas of wealth as unb稟ong and therefore criminal. One participant indicated:

“Crime is associated with mainly blacks, in most instances viewed to be a result of foreigners and the collection of these images might be reinforcing a stereotypical approach to crime fighting. Second, I have no idea who is collecting and analyzing the footage and what is the period of data retention. In the absence of enforcement provisions and powers of the Information Regulator until 2021, it means that there are few remedies, if at all.”

The final scenario, scenario five, presented issues of privacy and data protection in relation to gender identities and sexual orientation. The example used focused on how a privacy breach may expose someone's sexual orientation and the impact of location data being used to locate victims of gender-based violence. All the participants were aware of this as an issue. 90% of the participants were concerned about their privacy in this context and found this to be relevant to their area of work. For 95% of the participants, this was a concern and they wanted to know how to address this issue. The concerns with privacy breaches were related to how this information may be used. An example given was how women’s health information, if exposed to a data breach, may be used for problematic targeted advertisement. One of the participants indicated that a “privacy breach can also make someone susceptible to non-consensual intimate image sharing, online initiated human trafficking and kidnappings of women, children and sexual minorities.” Currently the sharing of non-consensual intimate images is addressed in the Film and Publications Act and the Cybercrimes Bill, 2017.

Key contextual issues that were recurring references were race, economic status, homophobia and gender-based violence. The issues around bias, discrimination and increased surveillance were raised as likely to be of concern as well. This led to questions of security breaches and their online safety given the sensitivity of their work. The concerns of safety and security were raised in the context of the high levels of gender-based violence in South Africa. Despite the rights of the LGBTQI community being protected, bias and discrimination will continue in these technologies with the reality of societal homophobia. In this instance the question of the extent to which anonymity can be guaranteed online is important.

As AI based solutions emerge, the concern with regards to gender is not necessarily a direct identification, but rather the emerging profiling and the targeted content based on that gendered profile. Even when data may be de-identified, algorithms may still be able to determine gender and sex life. Therefore, it is important to take necessary security safeguards that explicitly address these issues.

34 As above.
Privacy and data protection – assessing adequacy of the law

Data justice captures a wide understanding of social injustices and digital rights, but the focus of this paper is privacy and data protection. The concept of the right to privacy and data protection on the continent has steadily progressed over the last decade with laws developing at various times at national, sub-regional and regional level. The African Declaration on Internet Rights and Freedoms notes, accurately, that “many governments in Africa lack both the technical and legal resources to legislate appropriately and the political will to provide comprehensive protection to human rights in the context of internet and digital technologies.” 48 Where data protection laws do exist, they either replicate the European Union General Data Protection Regulations (GDPR), which has some interpretation challenges in itself, or they do not sufficiently protect and promote human rights and freedoms as they concentrate more on curbing cybercrime, terrorist activities or curtailing criticism of governments.

At a regional level, The African Union also published the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) which contains provisions that must be adhered to once it becomes legally binding. 49 However, only 14 countries have signed the document and only eight have ratified it which affects its adherence by member states. 50 At a sub-regional level in Southern Africa, The SADC Model Law on Data Protection (SADC Model Law) is a non-binding law developed as part of the Harmonisation of ICT Policies in sub-Saharan Africa (HIPSSA). 51 It was developed to provide guidance for purposes of data protection in the region. These laws do not explicitly refer to artificial intelligence related data issues nor are gender harms engaged with beyond the protected information category.

Despite much of South Africa’s AI and data-related policies and legislation being at a formative stage, the country’s existing regulatory framework has relevance to both the current governance of data and AI, as well as the conceptualisation and interpretation of new policies. In the Commission on the 4IR report, the increased use of data in these technologies is recognised as posing threats of large privacy breaches and likely to increase the surveillance capacity of government and firms in individuals’ lives. 52

The POPIA provisions relevant to the procession of personal information came into full effect in July 2020, with a 12 month grace period for compliance. Its provisions are framed in a way that ensures compliance for regional and global business practices and provides for the collection, processing and use of personal information. 53

Table 2 provides insights on principles guiding the POPIA which are some of the issues of concern related to artificial intelligence and the rights of people - referred to as data subjects. Section 71 speaks to automated decision making without human oversight, the only specific provision that directly speaks to AI.

---

**Table 2: Breakdown of some data protection principles**

<table>
<thead>
<tr>
<th>Relevant sections</th>
<th>Data protection principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition of personal information (section 1)</td>
<td>Personal information means information relating to an identifiable natural or juristic person such as their race, gender, sex, ethnicity, physical or email address, identity number, etc.</td>
</tr>
<tr>
<td>Definition of consent (section 1)</td>
<td>Consent means any voluntary, specific, and informed expression of will where permission is given for the processing of personal information. The processing of personal data is only allowed with the consent of the data subject or their parent or guardian if they are a minor.</td>
</tr>
<tr>
<td>Purpose specification (section 13)</td>
<td>Requirement that data be collected for a specific purpose; and, under section 18, the data subject must be notified when their data is being processed, must be able to access information on whether or not their personal data is being collected or processed, and must be able to object to the processing of their data.</td>
</tr>
<tr>
<td>Process limitation and minimality (section 10)</td>
<td>Personal information may only be processed if it is adequate, relevant and not excessive for the purpose it has been collected for. Further processing of information must be in line with the initial purpose of collection.</td>
</tr>
<tr>
<td>Data security (section 22)</td>
<td>A data subject and the data Regulator must be notified of any security breaches.</td>
</tr>
<tr>
<td>Retention (section 14)</td>
<td>Information must not be kept any longer than is necessary for the purpose it has been collected. This is subject to certain exemptions.</td>
</tr>
<tr>
<td>Right to erasure (section 24)</td>
<td>A data subject has the right to have their personal information corrected or deleted upon request.</td>
</tr>
<tr>
<td>Right to be informed (section 18)</td>
<td>A data subject has the right to be notified when their personal information has been collected and is being processed.</td>
</tr>
<tr>
<td>Provisions for automated decision making (section 71)</td>
<td>A data subject may not be subject to a decision with legal consequences solely based on automated processing of personal information.</td>
</tr>
</tbody>
</table>

42 Interview participants 3 and 4 interviewed in August 2020.
43 Survey respondent 1, 2020.
50 As above.
Gendered analysis of data protection - is it sufficient?

A gendered reading of the POPIA shows there is a need to unpack the gender harms generally related to privacy violations. Gender is not fully engaged with as a possible category of harm, rather it is sexual orientation which is considered sensitive data. There is need for the right to privacy and data protection to be ensured in a way that defines sensitivities and harms associated with intersex, transgender and diverse communities. 54 As Table 1 has shown these harms include discrimination, increased surveillance and reinforcement of negative gender stereotypes.

For a country that has constitutional provisions against discrimination on the basis of sex or gender, the language in the POPIA contains gendered pronouns which are discriminatory and exclusionary to people who do not identify as ‘he’ or ‘she’. The use of gendered pronouns has detrimental exclusionary consequences for sexual and gender minorities. The use of gender inclusive legal drafting is not a new phenomenon. Introduced by feminist movements as gender neutral language, it called for drafters of legislation and policy writers to avoid the application of masculine pronouns to the exclusion of women. 55 Today, gender neutral drafting is not only for the inclusivity of women. It requires that drafting be inclusive of gender diverse people. This includes the use of transgender-inclusive and non-binary inclusive language. In South Africa, the Cyber Crimes Bill 2017 is one of the laws which deliberates the inclusion of gender diverse people.

The law has also been criticised as being more responsive to global context rather than the lived reality within South Africa. An interview respondent highlighted that in the development of the POPIA, it is based on application of international best practices derived from the EU Data Protection Directive, 1995 and OECD Guideline on Data Protection and also takes into account common law and case law on the right to privacy. However, there is a need for more context specific nuances responsive to marginalised groups in society. As one respondent noted “one size fits all is not working so I would think that on a data privacy level, I would still stick to the fact that one should at least investigate as to how context would inform levels of privacy.” 57 In particular, respondents highlighted how the law was responsive to Eurocentric approaches of individualism in the protections of rights, yet there was a need to engage with the reality of community based harms – as is in the case of the experience of harms with AI based innovations.

In the context of gender and privacy, when laws do not consider gendered experiences, they overlook violations that may occur even when constitutional rights are enshrined. For example, an interview respondent highlighted that the lived reality of transsexual people may be particularly vulnerable to privacy violations when they do not fit into the cis normative gender box or their identity documents may not be reflective of the transition.

52 (n 29) 18.
55 Mulaudzi Mutondi ‘Feminism and the Law’ (Unpublished research).
56 As above.
57 Interview Respondent X interviewed in August 2020.
process they are going through in cases of identification (Interview respondent Q, August 2020). An example of this is cited in body imaging scanners that are used in public spaces such as airports. These are often designed with gender normativity in mind in the way in which they scan bodies and make use of risk algorithms to determine bodies that may be flagged for risk. 58

Data protection impact assessments that consider gender dynamics would be an important tool for ensuring data justice as well. This involves identifying, evaluating and addressing the impacts on data subjects and their personal data of a project, policy, programme or other initiative that entails the processing of such data. 59 In addition, states and non-state parties could provide easy access to data profiles and monitoring for gender bias. 60 Most algorithms are like black boxes and this impacts on understanding what is provided or incorporated. Principles of fairness, explainability, auditability, responsibility and accuracy should be infused. If this is done, it might reduce elements of bias. 60

While the right to be informed (Section 18 of the POPIA) on how the data will be collected and used within guiding principles, its implementation must be responsive to the power dynamics that would enable one to exercise agency and control. This is a challenge in AI based innovations where one is concerned with possible privacy intrusions yet uncertain on how to exercise these rights leading to a digital inequality paradox. The ability to exercise your rights online is dependent on awareness of the issue, digital skills, and literacy, and being able to meaningfully use the internet as well as understand how your data will be used. The concern is that without the ability to do this, one loses their agency over their own information. Thus, policy and regulation must take this into account to determine whether digital rights are being upheld or not.

Awareness must be complemented with responsibility to the technical community collecting, processing and using data to bear the cost and burden of explaining how the data is used in a way that is unequivocally understandable and considers accessibility barriers as well. In addition, the principle of privacy by design and data minimisation, that is collecting just the necessary data for processing, would be relevant with AI based innovations given that the impact is beyond the individual. As one interview respondent pointed out in their design solution dealing with sensitive issues – they designed the platform from a privacy by design perspective and collected the

“...So in this case we have to still do our best as a sector of technology makers, technology producers at best, kind of create this notion of collecting data. It’s our job to protect the users, it’s our job to make sure no matter what, even if they don’t engage, even if they don’t understand, their interests are protected. Especially if it comes to good or any technology for good.” 61

Civil society also has a significant role to play in ensuring the adequacy of privacy and data protection laws to respond to gender issues. Organisations such as the AmaBhungane Center for Investigative Journalism 62 and Right2Know have

60 As above.
61 Interview respondent Z interviewed in July 2020.
consistently worked towards holding the South African state and private entities accountable when it comes to increased surveillance of citizens from the state or private sector. Quite recently, Right2Know joined the case of Johannesburg Road Association against the roll out of CCTV cameras in Johannesburg. The premise of the case against the private company is that the company is spying on private citizens and has the intention to sell the data to third parties. However the focus on surveillance and privacy issues, needs to be nuanced in relation to the gendered impacts of surveillance and use of AI in surveillance systems. As interview participants pointed out, with the POPIA coming into effect, opportunities for strategic litigation will emerge that will nuance the gendered impacts of privacy violations.

The limitation of privacy and data protection laws stems from a general need to engage with the opportunities and challenges of AI based innovations and, at the same time, a lack of general engagement with gender and privacy issues.

63 Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186 (20 August 2020).
CONCLUSION

The current state of inequality in society affects women and the gender diverse communities adversely and this extends to the digital space. The narrative of AI for development and economic growth may overlook the reality of gendered inequalities and increase them further. By taking on a feminist conceptual framework this research has highlighted the challenges specific to women and gender diverse people in society overall and how this is a continuum with digital technologies. The development of AI follows the trend of excluding gender diverse people in the development and implementation of these innovations.

While it is commendable that the right to privacy is recognised and data protection measures are in place – the limitations in how gender is applied to the policies indicates the need for more engagement of gender in policy and law development. The review of gender specific harms related privacy and data show that a heteronormative and homogenous approach to policy is insufficient. Specific to AI – while the evidence on the continent is limited, the awareness and concerns drawn from the survey indicate there is a concern in the processing, collection and use of data and the subsequent harms as a result of the algorithm nudges on these platforms.

To be gender responsive means to design and implement policies that consider gendered realities of the society we live in and ensure that injustices are not replicated as we race towards digital development. The following recommendations are put forward on how this can be done with diverse stakeholders.

Recommendations:

Policy and regulation:

- Policy makers and regulators: Context based implementation and assessment of current and future privacy and data protection laws with regards to Artificial Intelligence innovations are necessary. The Information regulator and the Fourth Industrial Commission may be tasked with this role in collaboration with non-profit organisations for independent oversight. The current Artificial Intelligence Research institutions may be able to support technical understandings of the algorithms and automated decision-making systems currently in place.
- Policy makers and regulators: Capacity building of policy makers and the Information regulator and those whose work will be impacted by AI solutions will be crucial. Context based legislation is only possible when policy makers understand the issues and civil society has the capacity to hold them accountable.
- Breaking down silos in governance: There is a need for policy approaches that apply a holistic approach to governance instead governing issues in silos. Because of the way tech impacts the different aspects of life, industry policies and laws need to anticipate how governance of one issue or industry has an impact on another issue or industry.
- Oversight bodies: Monitoring and evaluation mechanisms such as gender audits of the law and AI initiatives can be implemented by the Commission on Gender Equality and the South African Human Rights Council in collaboration with the technical community. The proposed Artificial Intelligence institution would benefit from having
a gender chair tasked to support the oversight groups.

- Civil Society: Collaborative participation in future policy and regulatory design will be important to ensure context relevant approaches. Civil society and other stakeholders who are aware of the process of policy engagement may support submissions to policy processes or pull people and resources together to support public participation in policy processes.

- Civil Society and legal community: Strategic litigation to build up cases around gender specific harms will build necessary case law that may be used to support refinement of the current policy and regulation and in development of context based governance models.

- Resourcing: Adequate funding as well as staff capacity is necessary to ensure suggested measures may be implemented in a sustainable manner. This includes government adequately funding the Information regulator, supporting training initiatives for the cited oversight borders and funding of civil society adequately to build the necessary capacity to hold institutions accountable.

**Research and documentation**

- Case studies: Document the impact of existing policies on their respective constituents. Civil society and activists may actively engage in participatory action research to document experiences of their communities when it comes to AI based innovations and the emerging concerns of privacy breaches and adequacy of data protection.

- Governance models: Research for purposes of developing AI governance models that would ensure gender diverse people and sexual minorities may make use of their data to build AI systems responsive to their needs, have the ability to challenge AI based innovations and understand the process of AI innovations to hold innovators in public and private spaces accountable.

- Development of AI registrars: The extent to which Artificial Intelligence systems have proliferated South Africa, especially in the public sector is unknown. An AI registrar as done by the cities if Helsinki and Amsterdam would provide researchers and civil society a database to understand the take up of AI, how data is used, who has access to the information, the extent of human oversight and how the public has been made aware of the initiatives.

- Resources: Resourcing and funding would be needed to support research institutions in collaboration with civil society to conduct the research and build advocacy strategies. The funding provided should ensure outputs are accessible to the public in open source formats and engage with artists for creative communication.

**Public awareness:**

- Accessible information: Provide simplified information on policies regarding privacy and data protection in the national, regional, and global context. This may include developing guides in formats that are easy for users to understand and localised for language and cultural reference. The stakeholders involved would include government, civil society, and technical community.

- Public campaigns: Public awareness rooted in local communities and speak to people’s experiences of privacy and data issues online. Such campaigns can be implemented through partnerships with NGOs that operate on a national level and those that are rooted in communities with policy makers and digital rights activists. Community radios may be necessary avenues of prompting public discussions.

- Innovative communication: Innovative
and creative communications means through social media. Tiktok videos and videos that could be circulated through Whatsapp could have a wider reach. This may reach various age demographics active on these platforms. Working with youth organisations focused on gender and sexual justice issues would be key to developing context aware communications.

- Collaborative spaces: Creating spaces for context specific conversations as relating to the various issues various communities focus on e.g. women’s rights, LGBTIQ+, environmental rights, rights of the child and highlighting how they are all connected.

- Resourcing: Adequate resources would be needed to ensure the public awareness campaigns are conducted sufficiently and are sustainable. Government, technology companies and donors vested in gender and sexual justice may need to look to donating resources to supporting civil society to build on privacy and data protection to already existent public awareness campaigns.

Responsibility of technical community:

- Accountability: Public engagement and accountability reports on how AI algorithms are applied by these companies in society and whether they are responsive to contexts of inequality. The reports by companies must be in accessible formats with simplified languages. Transparency on these practices assists in documentation of challenges and opportunities with regards to data harms and may lead to increased trust of digital platforms.

- Ethical guidelines: Civil society and activists are in a great position to help draft ethical conducts and privacy with research institutes. Therefore, technical companies must collaborate with them to develop ethical guidelines that recognise the context and respond to gender and sexuality injustices because of AI based innovations. This would be most important for global technical companies that place regulations of privacy and data not relevant to the South African context.

- Digital literacy: The technical community - both local and international - must engage in digital literacy campaigns with marginalised groups to raise understanding of how the data they put out in the digital space is collected, processed and used. Technological companies must avoid hiding behind complexity and technical jargon to limit understanding of technology for users. The digital literacy campaigns must be done in a relevant language and a point of contact established for people to enquire about their data.

- Privacy and context by design: The technical community is encouraged to design and implement its AI innovations cognisant of the realities of marginalised communities in South Africa. Privacy practices should not be left as the responsibility of users alone, but developers should implement a privacy by design approach to ensure that when security breaches happen, marginalised groups are not adversely affected. The solutions must keep in mind the context of inequality, poverty, and unemployment so as to keep in mind the impact these solutions would have on society in this context.

Conflict of interest declaration: This research was made possible by a research grant from Mozilla foundation awarded to the researcher as a 2019/2020 Tech Policy fellow. The views expressed here are completely of the researcher.
Methodology

A feminist approach is used to assess the issues at hand beyond compliance for economic engagement, but rather the social aspects of the use of the technology within the context of social inequalities across the spectrum of gender and sexual identities. A feminist approach allows one to question who is being represented and by whom; whose interests are being centered; why this discussion is important and how it is taking place, which allows for criticism of power and how data itself can be used to ensure justice in society.

Table 3: A feminist conceptual lens

<table>
<thead>
<tr>
<th>Lens</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Feminism (Catherine D’Ignazio, Lauren F Klein)</td>
<td>7 guiding principles of data feminism</td>
</tr>
<tr>
<td></td>
<td>• Examine power</td>
</tr>
<tr>
<td></td>
<td>• Challenge power</td>
</tr>
<tr>
<td></td>
<td>• Elevate emotion and embodiment</td>
</tr>
<tr>
<td></td>
<td>• Rethink binaries</td>
</tr>
<tr>
<td></td>
<td>• Embrace pluralism</td>
</tr>
<tr>
<td></td>
<td>• Consider context</td>
</tr>
<tr>
<td></td>
<td>• Make labor visible</td>
</tr>
<tr>
<td>Feminist Principles of the internet</td>
<td>The principle of privacy and data that supports the right to privacy and full control over personal data and information online at all levels</td>
</tr>
<tr>
<td>Intersectionality (Kimberle Crenshaw, Patricia Hill Collins and Sylvia Tamale)</td>
<td>An understanding of social interactions with technology that consider multiple inequalities and locating technology in the context of systematic oppressions including racism, sexism, colonialism, classism, and patriarchy</td>
</tr>
<tr>
<td>Data Justice (Linnet Taylor; Data justice Lab and Global Data justice)</td>
<td>A way to center marginalised groups in datafied societies to recognise opportunities and respond to harms emerging from use of data in society that may have an adverse impact on groups in society.</td>
</tr>
<tr>
<td>Feminist internet ethical research practices</td>
<td>A feminist guiding tool with consent, accountability, respect, privacy, safety and reciprocity are the main ethical concerns of this study.</td>
</tr>
</tbody>
</table>

Guided by feminist epistemologies, data has been sourced through secondary and primary data which allow for multiple perspectives of knowledge. The secondary data draws from literature and an assessment of privacy and data protection law to assess its gender responsiveness. Through a process of mapping stakeholders from the data and a snowball methodology, a qualitative method of interviews was implemented in which ten individuals from the technical, academic, and legal community working on AI were interviewed. 65

66 See Table 4 for a profile of survey participants based on areas of work and community engagement.
A targeted survey, drawing from the snowball methodology of sampling drew responses from 25 activists working in the gender and sexual justice community. The approaches allowed for insight from these communities on their thoughts on AI within the South African context. It was not designed to be representative and therefore the finding may not be considered generic. They do allow for inferences and direction for further work.

Table 4: Profile of survey participants and communities of engagement.

Survey participants areas of work and community engagement

<table>
<thead>
<tr>
<th>Occupation</th>
<th>Area of engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research</td>
<td>Women and girls, LGBTIQ community, Disabled community, Sex workers</td>
</tr>
<tr>
<td>Media and communications</td>
<td>Women and girls, LGBTIQ community, Disabled community, Sex workers</td>
</tr>
<tr>
<td>Gender and Sexuality rights</td>
<td>Women, LGBTIQ community</td>
</tr>
<tr>
<td>Research</td>
<td>Women, Women and girls, LGBTIQ community</td>
</tr>
<tr>
<td>Tech policy and human rights</td>
<td>Digital rights issues.</td>
</tr>
<tr>
<td>Activism-Academia; Research</td>
<td>LGBTIQ community</td>
</tr>
<tr>
<td>Gender and Human Rights</td>
<td>Women, Working class communities, Migrants and undocumented communities</td>
</tr>
<tr>
<td>Marketing, branding and communications</td>
<td>Women, LGBTIQ community</td>
</tr>
<tr>
<td>Young women’s rights, digital rights</td>
<td>Women and girls, LGBTIQ community, Working class communities</td>
</tr>
<tr>
<td>Policy and Advocacy, Governance System</td>
<td>Women, Women and girls, Working class communities, Migrants and undocumented communities</td>
</tr>
<tr>
<td>Media</td>
<td>LGBTIQ community</td>
</tr>
<tr>
<td>philanthropy, civic space (online and offline)</td>
<td>Disabled community, Working class communities, Migrants and undocumented communities</td>
</tr>
<tr>
<td>Bookseller and Organiser</td>
<td>All of the above</td>
</tr>
<tr>
<td>Knowledge production</td>
<td>Women, LGBTIQ community</td>
</tr>
<tr>
<td>Business support services</td>
<td>Women, Women and girls, LGBTIQ community, Working class communities</td>
</tr>
<tr>
<td>Gender and research</td>
<td>Women and girls</td>
</tr>
<tr>
<td>Philanthropy and Human Rights</td>
<td>LGBTIQ community</td>
</tr>
<tr>
<td>Sexual and reproductive rights</td>
<td>Women, LGBTIQ community</td>
</tr>
<tr>
<td>Sexual and Reproductive services</td>
<td>Women, LGBTIQ community</td>
</tr>
<tr>
<td>Philanthropy</td>
<td>Women, Women and girls, Disabled community, Working class communities, Migrants and undocumented communities, children</td>
</tr>
<tr>
<td>Social Media</td>
<td>Women, LGBTIQ community</td>
</tr>
<tr>
<td>Community Manager</td>
<td>Women, Women and girls, LGBTIQ community, Working class communities</td>
</tr>
<tr>
<td>Feminist internet Research</td>
<td>Women, LGBTIQ community, Disabled community</td>
</tr>
<tr>
<td>Education - Human rights Law</td>
<td>Women, LGBTIQ community, Note: My research is technical and desktop</td>
</tr>
</tbody>
</table>
Bibliography

A Kovacs ‘When our bodies become data, where does that leave us?’ (2020) https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969 (accessed 28 September 2020);
Mulaudzi Mutondi ‘Feminism and the Law’ (Unpublished research).
M Onouha and D Nucera A People’s Guide to AI (2018) 8 and B Ricks and M Surman


Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC186 (20 August 2020).