# Understanding the Theory of Collective Rights: Redefining the Privacy Paradox

- **Commonly held truths surrounding privacy and data protection may negatively impact the design of effective policy and regulatory solutions.**
- **Debunking the privacy paradox in the context of public intersections with data subjects helps to highlight how individualized privacy self-management strategies are problematic as the sole (or chief) model for data protection.**
- **Identity projects, given the high level personal identifiable data required, are an important vulnerability context for considering new solutions on collective rights and protections.**

## Introduction

The protection of personal data is understood primarily as a privacy concern. Not only that, it is largely understood as a form of individual right, and an individual challenge. When considering how to protect this privacy in real ways, the first step is to consider the realities of *contextually specific* privacy challenges. Policy and regulatory solutions must not be constrained by atypical perspectives that exclude African realities in their design.

Debunking a central privacy trope, the 'privacy paradox', by confronting it with the context of public-sector driven identity projects in South Africa helps to uncover interesting nuances to the African data privacy perspective.

"The **privacy paradox** describes a supposed inconsistency between the concerns of people regarding **privacy** and their actual behaviour"

## Privacy paradox?

The privacy paradox is an important theory to understand in the context of privacy research, because it has dominated discussions on user behaviour in the field (and a strong analysis for solutions should of course root itself in understanding behaviours). While delving into the supposed paradox too deeply is not required, Solove notes there are two key perspectives for proponents and researchers on the topic:

1. In terms of the "behaviour valuation argument", the position essentially holds that because privacy is exchanged for low 'reward' (such as access to social media), it must mean people place low value on privacy; or

2. In terms of the "behaviour distortion argument", the behaviours of people in engaging in behaviour that violates their own privacy is irrational or inconsistent with what the actually want (Solove, 2020).

Many studies have been conducted on the 'paradox' (perhaps spurred by the relative ease for quantification comparing opinion to behaviour) and they frequently result in evidence of a "…mismatch between people's stated privacy concerns and their protective behaviours" (Bongiovanni et al., 2020).

Yet Solove refutes the existence of a paradox in its entirety, because of several generalisations they incorporate. The one generalisation is that a single decision taken by a user on a discrete piece of data can be extrapolated to reflect on their attitude to privacy in its entirety. but It cannot. And the other generalisation is that many privacy protections nevertheless remain in place when people 'exchange' their privacy in different consumer contexts, so to suggest a full trade-off of their privacy has happened is obviously false (Solove, 2020). Instead, failures to safeguard one's own privacy are rather because the processes for "privacy self-management" are insufficient (Solove, 2020).

Lessons gained from considering marginal user's engagement with biometric identity projects related to grant delivery in South Africa, in particular, also help to outline additional criticisms. The existence of the paradox necessarily presumes an exchange of equal bargaining power – after all, for the decision to 'relinquish' certain privacies to be deemed irrational, as the paradox requires, assumes there is a viable alternative path (it presumes a choice in fact exists). It presumes an existence of exchange which does not compute mandatory participation, nor participation that is *essentially* mandatory (because to not participate would severely impact the lives of the data subject). It presumes full agency.

A final key underlying assumption is that the risks and harms are individual, and thus the regulation and recourse should be fundamentally individualised. In other words, it suggests that the ultimate risks and harms need only be measured for the individual, rather than for any group, or collective, or a society as a whole. An examination of 'data exchange' in context will assist in fleshing out the inadequacies of this thesis.

# Considering the 'exchange'

On some level it may be deemed as unfair to critique consumerist perspectives on data privacy as being inconsiderate of public dimensions, given that the "privacy paradox" may *only be seeking* to engage on privacy in that form of exchange. Yet the reality is that a consumer-centred understanding of privacy has informed the trajectory of data protection legislation, even though the application of such law is far broader. And collectivist concerns for risks and harms extend to private-citizen data exchanges, as well (Tisne, 2020). Considering how data exchange may happen at a public sector interface provides a useful, and importantly particular, context for understanding the realities of privacy (Nissenbaum, 2009).

At their core, state identity projects state are an example of (largely) mandatory personal data exchange, increasingly requiring biometric data for deeply, and accurately, personally identifiable information (The World Bank, 2018). Depending on the context, they may be mandated by specific pieces of legislation, or instead, form part of digitisation activities of

pre-existing identity programmes (Bhandari et al., 2020). In countries like Mauritius and Kenya, there have been legal attempts to resist the lawful foundations of national identity programmes for different reasons,[1] but at a minimum they should be understood as *potential* intrusions into personal privacy given the data at stake.

Yet public sector collection of biometric data may not just be a part of national or civil registration projects, but might also be used as a way of facilitating access to particular services: in South Africa, the Department of Social Development has been engaged in biometric data collection to facilitate social grants distribution for well over two decades (Vally, 2016). This biometric function was in fact central to the South African Social Security Agency's selection in 2012 of a private service provider, Cash Paymaster Services, to help distribute grants (and collect biometric data in the process). That tender was successfully challenged in 2013, but social grants distribution was moved "inhouse", in partnership with the South African Post Offices, only in 2018.[2]

In 2018 in South Africa national statistics indicated 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). The reliance of these beneficiaries is an indicator not just of their income vulnerability, but also as a marker of their vulnerabilities across other markers of inequality and exclusion as well. As noted:

> "As people who have been 'watched by default', low-income populations in particular may be attuned to trading their details for welfare benefits" (Srinivasan et al., 2018).

People that infrequently use ICTs often only do so when compelled to in order to access services, and an additional barrier to equality in the experience of access to Internet more broadly is that the unaffordability of data, which is very consequential for lower-income groups usage, also means that "...most people are using services passively, not in the high-speed, always-on environment where studies of causality in relation to penetration and economic growth have been done" (Gillwald et al., 2018). There is a marked lack of agency in these contexts of 'exchange'. This is supported by evidence that digital interaction between citizens and government in South Africa in a *discretionar*y capacity is notably low, with fewer than 20 per cent of Internet users reporting that they use e-government services (Gillwald et al., 2018). This means that only a fraction of the South African population is readily accustomed to engaging government in a digital space with any form of autonomy.

These are not intrinsically unfair data collection activities. In fact, it is fundamentally important to highlight the many ways that increased visibility between South African citizens and the state helps to mitigate against decades of Apartheid exclusion. 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). Instead, what is being highlighted is that the notion that the 'data

---

[1] *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others* (Interested Parties) [2020] eKLR (Kenya); and *Madhewoo v The State of Mauritius & Another* 2015 SCJ 177 Mauritius).

[2] The chaos in relation to that tender, also known as SASSA-gate, was the subject of a myriad of litigation and also resulted in a plethora of risks to vulnerable citizens, outside of just privacy threats. One example of research done in the area that could be instructive is (Foley & Swilling, 2018).

subject' in this case is making an exchange of their privacy for a service (and income) seems a completely misguided rubric for seeking to understand the real nature of the interaction, and the actual power dimensions at play.

Reticence in populations to "prioritise" individual notions of privacy when handing over personal data – by say resisting biometric identity projects - may be a legitimate response to a history of exclusion through invisibility, and this social root is a peculiar history that must be understood. It may also be instructive to acknowledge the breadth of the right to privacy, which can be violated in South Africa not just by unlawfully processing true and correct personal data about an individual, but also by processing false and misleading data about an individual, with the former meaning a data subjects privacy is infringed and the latter infringing a person's individual identity (Naude & Papadopoulos, 2016). Identity, and its accuracy and preservation, are actually central to the notion of what it means to be a private individual.

# The reality of choice in theory

The ideas of exchange and choice, influenced by the consumer protection understandings of privacy, aren't sufficient for encapsulating how a citizen may engage with their own personal data, and privacy. Sociologists, and other scholars, have long explored interplays between agency and structure with far more dynamism. For instance:

> "The concept of structuralism…asserts that individuals do not make decisions based solely on rational choice. Their choices are shaped and influenced by political and economic organizational structures (such as governments and business organizations) — this is *independent* of their conception as to the legitimacy of such structures. In addition, there are social structures at play. These include sexism and racism, and class-based structures. While the relationship between individuals and the structures can be taken as a given, the extent to which individual action is dependent on structures is highly debatable…" [Emphasis added].(Ngcukaitobi, 2013).

These social and structural dimensions have seen expression in development economics, as well – with the capabilities approach noting that an individual's rights and freedoms (which include rights to privacy) are insufficient without the actual capability to achieve them (Sen, 2005).[3] This is not simply "an access to justice and process" capability (i.e. having place to act on your freedoms), but also having the resources (material and otherwise) to take opportunities to enact those freedoms (Sen, 2005). When we consider this understanding of freedom, and also the notions of structure, it provides more nuance to understanding if a data subject could have the capacity to say 'no'.

[3] Sen's own caveat that the capabilities approach and human rights are not analogous, though they are complementary, is of course acknowledged (Sen, 2005).

# Public privacy?

There is a final caveat, and that is understanding the rights (and capabilities) involved with privacy as solely individualised in their scope. Tufekci notes:

> "Data privacy is not like a consumer good, where you click 'I accept' and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices. A more collective response is needed" (Tufekci, 2018).

This is because when one person either sacrifices, or is forced to surrender, their privacy, the potential consequence of that is the exposure of collective (and not just individual) identity (Solove, 2020; Tisne, 2020; Tufekci, 2018). You can think of the extreme vulnerability in groups that may be the subject of identity programmes for, example, in refugee and immigration registration (Taylor & Meissner, 2020).

This collective appreciation also goes to the core of "valuing" privacy outside of economic understandings. While obviously a human rights perspective outlines a broader normative value, Solove notes the insufficiency of a purely economic perspective:

> "The fact that people share data in an age where it is nearly impossible not to do so has little bearing on the value of privacy"(Solove, 2020).

Just as the surrender of invisibility may have resource value to individuals, it should conversely be appreciated how the accumulation of that data can be marked by subjugation. 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). This social control can be politically motivated, or – in the exchange between data 'subject' and the private sector - commercially motivated (Zuboff, 2018). Yet both incentives, have the same resulting risk: maximising the exposure of the individual for exerting different forms of control over both the individual, and groups. A focus on individualised consent as *the* mechanism for the exercise of a freedom, in this political context, has one net result:

> "Consent without power leads to inequality" (Mhlambi, 2020).

When decisions on what is ethical privacy practice is determined solely by governments, or solely by the ethics of private companies, or (as in the case of the South African biometrics project cited) between holders of power of the public and private in collusion, the risks of simply reproducing existing political hegemonies (or amplifying them) continues (Razzano, 2020).

Instead, the collective value of privacy also helps to ground a regional perspective. For many years, the notion of personal privacy was seen as not prioritised in Africa as a rights area given its association to individualised, rather than communal, rights (Boshe, 2017; Razzano et al., 2020). For instance, the African Charter on Human and Peoples' Rights (1981) provides for a number of rights under the Universal Declaration of Human Rights, 1948 but does not mention the right to privacy. This omission is believed to have emanated from the perceived nature of the right by the framers of the African Charter, as promoting individualism contrary to the communalism that typifies African societies. Yet personal data protection

mechanisms are being instituted increasingly, and the right to access, update and correct personal information, which has its origins in the right to privacy, is protected in the Declaration of Principles on Freedom of Expression in Africa (Razzano, 2019). It may be more instructive instead to begin outlining the collective and relational aspects of the right to privacy. The value of protecting privacy go beyond the protection of the dignity of the individual (Burchell, 2009; Naude & Papadopoulos, 2016). The notion of ubuntu (the African concept '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).

# Conclusion

The true paradox of privacy may well be in the need to conceptualise it increasingly in terms of its public dimensions, rather than its personal ones. This is true for both broadening our understanding of how personal data is 'exchanged', to reconfiguring the inherent value of privacy, and also beginning to broaden our understanding of what effective remedies for breaches of privacy might be. Looking at personal data protection in the particular context of public-sector driven identity projects in South Africa demonstrates that the standard 'privacy paradox' provides little relevant perspective for trying to formulate policy and regulatory responses to data protection. Instead, there are structural and resource impediments which challenge the 'exercise' of privacy in context. And while of course no single policy can create the perfect enabling environment for all capabilities, it does highlight the need for creating access to recourse (such as through data protection authorities), but also more realistically for exploring mechanisms to ensure data protection more collectively (such as through data trusts or stewardships). Data protection cannot be fully realised through only ensuring privacy in consumer exchanges, given the role of the public sector and public-private partnerships, but also the remit for collective action needs to be explored more broadly in order to preserve privacy's true values.

_____

*To subscribe to RIA's newsletter, sign up here.*

**Author**

Gabriella Razzano

**Enquiries**

info@researchictafrica.net

Workshop 17, Watershed, Cape Town

T: +27 214476332

W: www.researchictafrica.net

# References

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

Bongiovanni, I., Renaud, K., & Aleisa, N. (2020, July 29). *The privacy paradox: We claim we care about our data, so why don't our actions match?* The Conversation. http://theconversation.com/the-privacy-paradox-we-claim-we-care-about-our-data-so-why-dont-our-actions-match-143354

Boshe, P. (2017). *Data Protection Legal Reform in Africa*. Passau University.

Burchell, J. (2009). The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law*, *13*(1). https://www.ejcl.org/131/art131-2.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

Foley, R., & Swilling, M. (2018). *How One Word Can Change the Game: Case Study of State Capture and the South African Social Security Agency* [State Capture Research Project]. Centre for Complex Systems in Transition, Stellenbosch University.

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

Gillwald, A., Mothobi, O., & Rademan, B. (2018). The State of ICT in South Africa. *Series 5: After Access*, *5*. https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf

Mhlambi, S. (2020). *From Rationality to Relationality: Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance* (Carr Centre Discussion Paper). Harvard Kennedy School. https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial

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.

Ngcukaitobi, T. (2013). Strike Law, Structural Violence and Inequality in the Platinum Hills of Marikana. *Industrial Law Journal*, *34*, 836–857.

Nissenbaum, H. (2009). *Privacy in Context*. Stanford University Press.

Razzano, G. (2019). Human rights dimensions of digital trade. In *Digital Trade in Africa: Implications for inclusion and human rights* (pp. 61–70). United Nations Economic Commission for Africa, Office of the High Commissioner for Human Rights and Friedrich-Ebert-Stiftung. https://www.uneca.org/sites/default/files/PublicationFiles/dthr_en_full_rev3.pdf

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

Razzano, G., Gillwald, A., Aguera, P., Ahmed, S., Calandro, E., Rens, A., & Spuy, A. van der. (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/

Sen, A. (2005). Human Rights and Capabilities. *Journal of Human Development*, *6*(2), 151–166. Academic Search Premier. mlzsync1:0041{"extrafields":{"publisher":"Routledge"}}

Solove, D. (2020). *The Myth of the Privacy Paradox*. http://scholar.google.co.za/scholar_url?url=https://scholarship.law.gwu.edu/cgi/viewcontent.cgi%3Farticle%3D2738%26context%3Dfaculty_publications&hl=en&sa=X&ei=yfoPYNuQAfGTy9YPt-iH6A4&scisig=AAGBfm3wK8BCeq6t4dsxDd71kYvjYG_wyA&nossl=1&oi=scholarr

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.

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

Taylor, L., & Meissner, F. (2020). A Crisis of Opportunity: Market-Making, Big Data, and the Consolidation of Migration as Risk. *Antipode*, *52*(1), 270–290. https://doi.org/10.1111/anti.12583

The World Bank. (2018). *Principles on identification for sustainable development: Toward the digital age* (No. 112614; pp. 1–20). The World Bank. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age

Tisne, M. (2020). *The Data Delusion: Protecting Individual Data Isn't Enough When the Harm is Collective*. Stanford Cyber Policy Centre. https://cyber.fsi.stanford.edu/publication/data-delusion

Tufekci, Z. (2018, January 30). The Latest Data Privacy Debacle. *The New York Times*. https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html

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

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