



“To Digital ID, or Not to Go Digital, That is the Question”

Digital Identity In South Africa: A
Discussion Paper (November 2025)
Version 1.0

ABSTRACT

This paper examines the South African government’s proposed Digital Identity (DID) system within the *MyMzansi* Digital Public Infrastructure initiative. While outlining potential benefits such as improved access to services and fraud prevention, it raises serious concerns around privacy, surveillance, exclusion, and government overreach. Drawing from legal analysis, real-world experience, and the Liberty Fighters Network’s position, the paper advocates for a voluntary, rights-based approach that respects constitutional freedoms and ensures no citizen is coerced or left behind.

Reyno De Beer
LFN President

www.libertyfighters.org

Table of Contents

Summary	1
Introduction	2
Legal and Privacy Considerations	3
The Liberty Fighters Network Perspective on Trust and Government	6
Potential Benefits of Digital IDs	8
Concerns and Risks of Digital IDs	10
Balancing Rights and Options for Citizens	15
Conclusion	17
Sources	18

Summary

This discussion paper critically explores South Africa’s proposed Digital Identity (DID) system within the broader *MyMzansi* Digital Public Infrastructure (DPI) initiative. It assesses the potential benefits, risks, and socio-legal implications from the perspective of the Liberty Fighters Network (LFN), a civil society body known for its stance on personal liberty, digital rights, and opposition to state overreach. The paper outlines the legal framework under the **Protection of Personal Information Act, 2013 (POPIA)**, the **Financial Intelligence Centre Act, 2001 (FICA)**, and the **Consumer Protection Act, 2008 (CPA)**, questioning whether current legislative protections are adequate for a biometric-driven, state-administered identity system.

While acknowledging possible benefits such as improved service delivery, fraud prevention, and convenience in emergencies and international travel, the paper warns of significant risks, including surveillance, data breaches, systemic exclusion, and function creep. The document situates these concerns in a context of public distrust, historical misuse of identity systems, and perceived government corruption. It incorporates lived experiences and raises the alarm about potential future scenarios

where access to services, freedoms, and even democratic processes like voting could be digitally restricted or manipulated.

The paper advocates for a dual-system approach that preserves citizens' right to opt out, emphasises public accountability, and calls for robust legal safeguards. LFN urges that any rollout of DIDs be voluntary, transparent, and constitutionally compliant to avoid repeating the mistakes of past control systems under a modern digital guise.

Introduction

South Africa is on the cusp of a major shift in how personal identification is managed. The government has announced plans to develop a national digital identity system that would provide each citizen with a single, unified credential for accessing services across multiple sectors[1]. This initiative is part of the broader *MyMzansi Digital Public Infrastructure (DPI)* blueprint, which envisions a seamless digital government platform. According to Communications Minister Solly Malatsi, the future of government services lies largely in rolling out a single digital ID through MyMzansi's infrastructure[2]. The MyMzansi mobile app will serve as a central portal where South Africans can log in with a unique digital identity to access various government services[3]. Notably, the app is planned to be zero-rated (no data costs for users) and will use biometric verification – for example, facial recognition – so that citizens can authenticate themselves remotely[3].

Biometric face recognition is a key component of the proposed digital ID system, allowing identity verification via smartphone[3]. The MyMzansi app will let citizens store ID cards, passports, and other documents digitally for convenient access to public services[4].

The push for a digital ID is motivated by several factors. Authorities argue that a unified digital identity could streamline service delivery, reduce fraud, and improve security[5]. Currently, South Africans must manage multiple identifiers – from ID numbers to tax,

business, and medical scheme numbers – which creates duplication and opportunities for fraud[6]. For instance, as former SARS Commissioner Edward Kieswetter noted, one person can exploit disconnected systems by using different identities to draw benefits like social grants while employed, simply because the databases aren't linked[6]. A single digital ID (potentially combined with a physical smart card) is presented as the answer to these issues, with officials even pointing to India's successful *Aadhaar* biometric ID program as a positive example of what a unified ID can achieve[7]. The South African Reserve Bank, SARS, and the Department of Home Affairs are collaborating on this project, underscoring its importance across government departments[1].

It is important to acknowledge the historical context that makes any new identification system in South Africa a sensitive topic. Identity documents were a tool of control during the era of racial segregation (a system originally engineered under British colonial rule, and commonly known by its Afrikaans name *apartheid*). This legacy means many citizens are inherently wary of new ID systems that could centralize personal data and potentially be used to control or segregate populations. With that in mind, this discussion paper examines the potential benefits of digital IDs (sometimes referred to as DIDs) as well as the risks, legal issues, and societal implications from the perspective of concerned civil society observers, notably the **Liberty Fighters Network (LFN)**. LFN is a group that has been vocal about civil liberties and government overreach, and their perspective provides a critical lens through which to evaluate the digital ID initiative.

Legal and Privacy Considerations

Any digital identity system must operate within South Africa's legal framework for privacy and consumer protection. The POPIA establishes important principles for processing personal data[8]. POPIA is intended to safeguard citizens' personal

information and govern how both private companies and government entities handle that data. However, POPIA on its own may not be fully adequate to regulate a nationwide government-run digital ID system – it was primarily oriented toward private-sector compliance, and *administrative uses of biometric data raise distinct concerns that POPIA doesn't explicitly address*[8]. For example, if the digital ID system uses fingerprints or facial recognition data, how long will this biometric data be stored, who can access it, and what happens if it's compromised? These questions highlight the need for robust oversight and possibly additional legislation to put guardrails around the use of digital IDs by the state[9][10]. Some legal experts have even suggested creating a dedicated Administrative Data Protection Act to supplement POPIA for government applications of biometric ID systems[11].

Another relevant law is the FICA, which underpins the “know your customer” requirements in banking. FICA was enacted to fight financial crime such as money laundering, fraud, tax evasion, terrorist financing, and even identity theft[12]. Banks often cite FICA compliance when they require customers to provide identification and proof of address. In practice, many South Africans are already accustomed to stringent ID checks for opening bank accounts or buying mobile phone SIM cards (due to FICA and RICA laws). A digital ID could streamline these compliance processes, theoretically making it easier for banks to verify identities. However, questions arise when private institutions start making a digital ID the only way to access services. For instance, if banks or retailers make it compulsory to use the new digital ID for transactions, one must ask: *Is that legal under our consumer protection laws?* The CPA guarantees consumers the right to choice and fair, non-discriminatory treatment. Forcing customers to use a specific digital platform or ID could be seen as limiting their choice, especially if alternative methods (like physical IDs or bank cards) are curtailed. It remains an open question whether making a digital ID effectively mandatory in commerce would contravene the CPA's provisions – this is an area where regulatory clarity is needed. Even if banks strongly encourage the digital ID for convenience or security, they would need to ensure they are not infringing on consumer rights by penalizing those who still opt for traditional identification methods.

Privacy is a central concern as well. A unified digital ID means a lot of personal data could be linked in one place – from health records to financial information and travel history. Without proper safeguards, this concentration of data raises the risk of abuse. South Africans have recently expressed fears online that a digital ID system could enable the government to track people’s movements and even cut off access to basic services at the press of a button[13][14]. Such fears might sound extreme, but given the country’s history and current levels of mistrust, they resonate with many. It is worth noting that many of these capabilities (tracking, denial of services) already exist to some degree under the current systems – for example, your movements can be tracked if you use bank cards or cellphones, and the state can block ID books in cases of identity fraud[13][15]. The difference, critics argue, is that a fully digital ID could make such surveillance or control instantaneous and more pervasive, with decisions potentially made by algorithms rather than humans. This is why transparency and accountability in how the digital ID is managed are crucial. Citizens will need assurances that their data is secure and that there are checks and balances preventing any unwarranted snooping or arbitrary denial of services.

POPIA does give individuals some rights over their personal information, such as the right to be notified about data collection and the right to request deletion or correction of data. How will these rights be implemented in the context of a government digital ID? For example, can a citizen opt out of certain data being linked to their ID, or challenge an automated decision (like a biometric match failure) that affects their access to services? Without clear answers, the legal robustness of the system remains in doubt. LFN and other civil rights advocates would likely push for any digital ID rollout to come with strong privacy protections, independent oversight, and remedies for individuals who feel their rights have been infringed by the new system.

The Liberty Fighters Network Perspective on Trust and Government

LFN has been one of the vocal organisations scrutinising government initiatives like the digital ID. LFN's scepticism toward the digital ID is rooted in a broader distrust of government overreach. This distrust was heightened during the COVID-19 "pandemic": LFN openly opposed the government's COVID-19 measures and lockdown regulations, and it has been *categorically against vaccination mandates* or any form of required vaccination status. In fact, LFN opposes the idea of having to declare one's vaccination status at all, viewing it as a dangerous precedent for personal freedom. This stance emerged from their fight against what they perceived as unconstitutional restrictions during the lockdown, and it carries over into how they view centralised digital identity systems. From LFN's perspective, a digital ID could become a platform for enforcing medical decisions (like proof of vaccination) or other policies they vehemently disagree with.

LFN's mistrust of government intentions runs deep and is shared by many South Africans who feel let down by years of corruption and poor governance. When the government pitches a new high-tech ID system as a solution for efficiency, LFN supporters ask "*Solution for whom?*" There is a prevailing sentiment among opponents that "*everything coming from the government is suspicious, notwithstanding even if the intentions were sincere*". This climate of mutual mistrust means that even if the digital ID plan is genuinely meant to improve service delivery, many will suspect a hidden agenda of control.

One often-cited fear is that digital IDs are really about social control and surveillance. LFN members frequently assert that a digital ID is "all about control" rather than convenience. They argue that a corrupt government could use the system to keep tabs on political dissidents, restrict rights, or favour the elite. For example, *who gets access to the data?* Could law enforcement or intelligence agencies use the digital ID database

to monitor citizens without due process? South Africa has seen surveillance tools expanded in the name of security before. A case in point: the installation of CCTV cameras in public areas. I have personal experience in this domain – I was involved during 2002 in *launching* the first public CCTV surveillance system making use of facial recognition technology in the Sunnyside area as part of a community safety initiative. The official reason was to combat rampant crime in that neighbourhood, and indeed such powerful CCTV can be a useful crime-fighting tool. However, many of us observed anecdotally that while crime might have shifted or become more covert, the cameras also ended up serving other interests. Some in LFN wryly remark that *our government is so corrupt it installs CCTV to monitor other criminals* – in other words, *the state (viewed by LFN as itself corrupt due to its representatives being corrupt) wants to keep an eye on potential rivals in crime*. It's a cynical take, but it reflects the depth of distrust: even crime prevention measures are seen as potentially self-serving for a corrupt elite. There's even the dark reality that crime has become South Africa's biggest industry, also convenient for those in power who benefit from security contracts and a culture of fear. In the narrative LFN presents, a digital ID could become yet another part of this surveillance tapestry – a tool the government sells as security but potentially uses to tighten its grip on citizens.

This perspective is bolstered by LFN's stance that DIDs (digital IDs) primarily benefit a "corrupt elite" rather than ordinary people. LFN supporters believe that if you follow the money and power, the ones who stand to gain from every citizen being digitally tagged are those already in control – whether in government or big corporations aligned with the state. They worry that the digital ID could become like a *digital "dompas"* (reference to the infamous passbooks of the segregation era) that citizens must produce on demand, and which could be turned off for anyone who falls out of line. It's a dystopian scenario, but one that resonates given past abuses of ID systems in South African history.

It's worth noting that this mistrust is not simply irrational paranoia; it's born from experience. South Africa's governance issues – from high-profile corruption cases to

failure in service delivery – naturally make people hesitant to hand over more power (and personal data) to the state. LFN, for its part, has positioned itself as a watchdog and activist group that often works independently. They don't readily trust many organisations or political parties either, preferring not to ally too closely with others who might dilute their stance. (In fact, if any comparisons have been made between LFN and mainstream opposition parties, LFN would reject that; their anti-establishment approach is not on par with conventional politics.) That said, LFN isn't entirely isolationist – they remain open to collaborating strategically (“we possibly may ally with others”) if it means protecting citizens' rights. But any partnership would have to share LFN's scepticism of centralised power and commitment to individual freedoms.

In summary, from the LFN point of view, a digital ID system is guilty until proven innocent. Their baseline is that such a system will likely be used to *increase state control, harvest personal data, and serve the interests of a few at the top*, unless strict measures are in place to prevent that.

Potential Benefits of Digital IDs

While LFN and others highlight many concerns, it's also important to discuss the potential advantages of a digital identity system (if it is innocent) — some of which even sceptics might cautiously acknowledge:

- **Convenience and Security of Not Carrying Physical Documents:** A digital ID could let people prove their identity or qualifications using just their smartphone, reducing the need to carry ID books, driver's licenses, bank cards, or certificates. For example, a secure app could store your ID, passport, and even credit cards in one place^[4]. This would be very handy in daily life and eliminate the risk of losing important documents. *(On a personal note, I experienced this first-hand when my wallet (a small moon bag) was stolen. Cancelling cards and replacing my ID was a major hassle. The idea that I might not need to carry those cards at*

all – that they could be securely on my phone or hidden by my fingerprint – is hugely appealing.) The convenience factor of DIDs is undeniable. Imagine traveling domestically without worrying about forgetting your driver’s license, or proving your age with a tap on your phone instead of carrying an ID book.

- **Rapid Verification and Access to Services:** Digital IDs can speed up processes like opening a bank account, or applying for government services. Biometric verification (like a selfie scan or fingerprint) can instantly confirm your identity from anywhere. The government touts that this will make services more efficient and cut down on queues and paperwork[5]. For instance, the South African Revenue Service (SARS) has already introduced facial biometric checks for online tax filing registration[16], which hints at how a broader digital ID system could streamline many interactions. Efficiency also means fraud prevention – it’s easier to catch someone trying to use a false identity when verification is tied to biometrics and a single national database (reducing the “duplication” issue Kieswetter described[6]).
- **Help in Emergencies or Travel:** A digital ID could be a lifesaver if your physical documents are lost or stolen while traveling. Picture being abroad and losing your passport – if you had a verified digital ID, an embassy might reissue credentials faster, or airlines might accept the digital ID to let you fly home, thanks to secure verification. Even domestically, if your bank card is stolen, having a digital wallet ID could allow you to freeze accounts and prove your identity to your bank without needing to go into a branch with a physical ID. The advantage for international travel is significant: some countries are exploring digital passports or vaccination certificates (with which LFN has a major problem); having our own interoperable digital ID could smooth out identity checks at borders or when dealing with foreign authorities, provided international standards are met.
- **Financial Inclusion and Innovation:** Proponents argue that a digital ID system could include more people in the formal economy. Millions of South Africans, especially in rural areas, lack easy access to banks or government offices. If they had a digital ID and a mobile phone, they could potentially sign up for services

remotely that were previously out of reach. This ties into the idea of digital public infrastructure – with a reliable ID, people could access grants, register businesses, or transfer money without needing to travel long distances. There’s also an innovation angle: fintech companies and startups could build services on top of the digital ID platform (with permission), potentially offering new solutions for payments, credit, or healthcare that are secure and tailored to verified users. The government has indicated that along with digital ID, things like digital payments systems are on the roadmap[17], which could modernise the economy.

It’s clear that even for those of us who are cautious, *not carrying physical cards and IDs around, and having a backup if they’re stolen, would be very convenient. But at what cost does this convenience come?* To reap these benefits, citizens would be entrusting a lot of sensitive data to the government’s systems and would become more dependent on digital infrastructure in daily life. This is why we must weigh the benefits against the potential costs discussed in the next section.

Concerns and Risks of Digital IDs

Despite the potential benefits, the introduction of digital IDs in South Africa raises a host of concerns and risks. These need to be carefully considered and addressed to avoid unintended consequences. Here are some of the key issues identified by LFN:

- **Government Surveillance and Abuse of Power:** Perhaps the biggest fear is that a digital ID will give the state unprecedented visibility into citizens’ lives. If every activity – from banking to medical visits to travel – is tied into one ID system, a bad actor in government could theoretically monitor or control people with a few keystrokes. LFN warns that what is pitched as a tool for convenience could morph into a tool for oppression[14]. They point to scenarios like authorities cutting off a person’s access to services (financial services, driver’s license, etc.) if that person is deemed problematic, effectively “cancelling” someone’s

existence with the flip of a switch. While similar control is possible with the existing ID system, a digital one could make it *instant and automated*. Moreover, given South Africa's corruption issues, sceptics worry that surveillance might not even be for lawful purposes – it could be used to track political opponents, activists, or even to protect corrupt interests (as suggested by the concerned view of CCTV being used by government to watch “other criminals”). Strong oversight and legal safeguards would be needed to prevent any such abuse, but the trust in government to self-police is very low.

- **Privacy and Data Security:** A central database (or interconnected databases) of digital IDs would be a highly attractive target for hackers and a rich repository of personal data. A breach could expose millions of people's personal information, far worse than any single credit card hack. Furthermore, even internally, there's concern about how data might be shared between departments. *Will tax, health, and home affairs data all be linked?* Citizens might not want their health records, for example, to be readily accessible by a host of government agencies or officials. Under POPIA, data minimisation and purpose limitation are principles that should restrict such sharing[8], but enforcement in a massive system can be tricky. The biometric aspect adds another layer of concern: if your fingerprint or face print gets stolen (*via* a database leak), you can't exactly change those like you would a password – that identity marker is compromised permanently[18]. The government will need ironclad cybersecurity and clear rules on data access to mitigate these risks, but no system is fool proof. Privacy advocates will likely push for measures like encryption, decentralised storage of certain credentials, and transparency reports on how often data is accessed or shared. Without convincing answers on how citizens' personal information will be protected, many will remain uneasy about digital IDs.
- **Exclusion and Inequality:** Ironically, a system meant to include everyone can end up excluding some of the most vulnerable. South Africa has a large population that still lives in rural areas, some in deep poverty, and a number who deliberately stay “off the grid”. It's estimated that millions of people do not even own a basic cellphone (like an old Nokia 3310), or they live in areas with poor

connectivity. How will a digital ID accommodate people with no smartphones or internet access? If the government moves many services to the digital platform and closes down paper-based or in-person alternatives, those citizens could be left stranded. There's also the issue of digital literacy – some may have phones but not know how to navigate a new app, especially elderly citizens. The Department of Home Affairs has indicated the system will include both physical and digital components (likely to account for some of these issues)[19], but the rollout must be very careful not to marginalise those who can't easily go digital. Moreover, there are real-life cases in South Africa where people have effectively lived *outside* the official ID system. I am aware of instances where parents never registered their children at birth, whether due to ignorance or choice. These individuals grew up as “*citizenless*” adults – with no ID number, they cannot legally work, open bank accounts, or even get a library card. One might think being invisible to the state is a kind of freedom, but in truth it is a harsh existence. Such people live as paupers on society's fringes, often relying on friends or family members to do any official transactions on their behalf. Their lack of identity is a prison of a different sort – arguably worse than being known to the system, since they can't access opportunities or rights at all. This scenario is a cautionary tale: *not having any recognised ID can be catastrophic for one's life chances*. We must ensure the digital ID system doesn't inadvertently create a new class of “digital exclusion” where those who don't, can't, or won't join are left with virtually no life in the modern society. International experiences also sound warnings: researchers note that digital ID systems, if poorly implemented, can amplify existing inequalities[20]. For example, Uganda's digital ID (Ndaga Muntu) reportedly *locked out thousands of women and elderly people* from receiving services when they couldn't get registered in the new system[21]. We absolutely need to avoid such an outcome here.

- **Misuse for Unrelated Purposes (Function Creep):** Another concern is that once a digital ID is in place, it might be used for more and more purposes beyond its original intent – a phenomenon known as *function creep*. For instance, while the current justification might be fighting fraud and easing service access, later

the ID could be required to log into social media, or to make everyday purchases, creating a comprehensive tracking tool. LFN specifically fears the incorporation of things like vaccination status into the ID. During COVID-19, there was global talk of “vaccine passports”. Imagine if in a future scenario the government decided that your digital ID must show your vaccination records for you to enter public buildings or travel. LFN and its supporters, staunchly anti-mandate, would see this as a nightmare – effectively turning the ID into an enforcement mechanism for health policies they don’t trust. Even beyond health, there’s worry about political or financial coercion: could the digital ID be used to implement a social credit system or to automatically fine people for debts and tickets by linking to their bank accounts? These ideas might sound far-fetched, but they are the kinds of slippery slope uses that make people nervous about giving the state a powerful tech tool.

- **Democratic Implications (e-Voting and Civil Rights):** One particular application of digital IDs that divides opinion is electronic voting (e-voting). On one hand, a secure digital ID could enable citizens to vote online in elections, potentially increasing turnout and making voting more accessible. On the other hand, LFN and many others are adamant that *we must prevent e-voting*, believing that nothing beats a proper physical paper ballot system for transparency and fraud prevention. Given South Africa’s contentious politics, the integrity of elections is paramount. Those wary of e-voting fear that digital votes could be manipulated or that lack of a paper trail would undermine trust in the outcomes. If the digital ID system is seen as a stepping stone to e-voting, expect fierce resistance on that front. There’s also a broader civil rights question: Will participating in protests or joining certain groups be quietly recorded *via* digital IDs? For instance, if an e-voting or e-petition platform requires your digital ID, your political activities become part of your data profile. In a healthy democracy this might not be abused, but in a fragile one it could be. Hence, protecting anonymity and the right to dissent is another concern tied to how the digital ID is designed.

- **Uncertain Redress and Governance:** Finally, a practical risk is the governance of the ID system itself. If something goes wrong – say the system flags you incorrectly as deceased or as a fraud suspect – how quickly can it be corrected? In the analogue world, one could go to Home Affairs and argue their case; in a digital automated world, that might be harder if “the computer says no”. There must be clear, quick avenues for people to appeal and fix errors (e.g., a way to unblock an ID or update info without lengthy bureaucratic battles). Additionally, who oversees the overseers? An independent ombudsman or data protection authority should be empowered (and resourced) to audit the system, handle complaints, and penalise misuse. LFN and others would likely demand strong accountability mechanisms to be built in from the start. Otherwise, any promises made about how the system will be used could be broken quietly, with citizens none the wiser.
- **Double Standards and Transparency for All:** A poignant question raised by sceptics is whether the same transparency and traceability will apply to powerful institutions as it will to citizens. If every person’s transactions and interactions become more traceable through digital IDs, will we also get more transparency into, say, what banks and large corporations are doing? For example, would the digital infrastructure make it possible to trace banks’ own complex financial practices (like securitisation of loans and investments) so regulators can easily spot corruption or illicit flows? Or will the surveillance remain a one-way street aimed only at the populace? Many fear that without equal scrutiny of the elite, digital ID systems simply extend the imbalance of power. For trust to be fostered, the government would need to show that digital governance isn’t just about watching ordinary citizens, but also about shining a light on institutional malfeasance – essentially, *trust is a two-way street*. If the public sees that digital tools are also used to catch high-level corruption and not only to police the little guy, some confidence may be gained. Right now, however, LFN supporters doubt that the architects of the system have any intention of applying it to themselves or their powerful allies, which feeds the narrative that DIDs are only there to benefit the corrupt elite and keep tabs on everyone else.

In summary, the concerns span from technical and legal issues to deep-seated societal trust issues. South Africa is not alone in these debates – globally, digital ID initiatives have sparked fierce discussions about striking the right balance. As one group of researchers observed, *digital IDs aren't neutral; they come with both promise and peril, and outcomes depend on design and implementation choices*[22]. We must learn from other countries' mistakes and our own past when bringing any new ID system into being.

Balancing Rights and Options for Citizens

Given the benefits on one side and the serious risks on the other, the big question is how South Africa can move forward in a way that respects citizens' rights and choice. One idea gaining traction is to **make digital IDs optional** – effectively running a dual system. In such a scenario, those who are comfortable and see the value can adopt the digital ID, while those who prefer to live “off the grid” or stick to traditional methods can continue to do so without penalty. This dual-system approach would acknowledge a reality we face: we have a diverse population with different needs and trust levels. Some urban, tech-savvy citizens might love the convenience of a DID, whereas others in rural or privacy-conscious communities might choose to opt out. *Accommodating both could be key to social acceptance.* If South Africa's government forced everyone to use the digital ID for all interactions, it could create backlash and non-compliance that undermines the whole project. By contrast, a **voluntary adoption model** could build trust by proving the system's value to those who use it while not alienating those who are hesitant.

However, running a dual system is not without challenges. It can be costly and complex to maintain parallel processes (digital and physical) for things like grant payments or license renewals. The government might argue that it defeats the purpose of efficiency. A potential compromise is to ensure *no one is denied essential services due to not*

having a digital ID. Perhaps make the digital ID advantageous (faster service, maybe certain discounts or added security features) but still provide “offline” channels for every government service. Over time, if confidence grows, more people will naturally migrate to the digital platform. But **force should not be the strategy** – especially not at first. South Africa’s Constitution protects the rights to equality and to administrative justice; if people who don’t use digital IDs start being treated as second-class citizens, that could raise constitutional issues.

Transparency and public engagement will also be crucial in balancing this transition. The government should be open about what the digital ID does and doesn’t do. Continuous public dialogue (with groups like LFN, other NGOs, tech experts, and ordinary citizens) can help refine the system and address fears. Perhaps establishing a citizen oversight committee or involving civil rights groups in the planning can improve credibility. At the end of the day, trust has to be earned. The *onus* is on the state to prove that a digital ID will serve the people and not harm them.

Additionally, strengthening legal protections can go a long way. For example, updating the CPA or issuing regulations to clarify that no private company can exclusively force digital ID usage without offering alternatives would protect consumer rights during the transition. Passing those “legal guardrails” (like the suggested Administrative Data Protection Act)[11] for government use of digital IDs would show commitment to avoiding abuse. If citizens see that there are robust laws giving them control and recourse (like the ability to sue or claim damages if their data is misused, or if they are unfairly excluded by the system), they might feel more at ease.

Another aspect of balancing rights is addressing the digital divide head-on. The government will need initiatives to provide access and devices to those who lack them if it ever expects near-universal uptake. Perhaps subsidies for basic smartphones, or government-funded digital kiosks in rural areas where people can log in with assistance. If someone in a village doesn’t have signal or a smart device, maybe a local post office or community centre could serve as a digital ID touchpoint (much like ATM or banking

agents). These kinds of accommodations would demonstrate that no one is being left behind or coerced.

Lastly, **maintaining the integrity of democratic processes** is non-negotiable. If any part of the digital ID plan in the future hints at integrating with voting, it must be debated thoroughly with all stakeholders. LFN and others will fight tooth and nail to keep voting a manual, auditable process – and for good reason. Perhaps a middle ground could be considered where digital ID is used for voter registration or identification at polling stations to prevent fraud (replacing the current green ID book checks), but the actual casting of votes remains on paper ballots. That could improve election security without introducing the spectre of electronic vote tampering.

Conclusion

The introduction of digital IDs in South Africa is a complex, multifaceted issue that touches on technology, law, society, and trust. On one hand, there is a clear trajectory toward digital transformation – the government is embracing it as part of modernising service delivery, and many citizens could benefit from the convenience and efficiency it offers^{[2][5]}. On the other hand, our country's unique history and current challenges mean that a one-size-fits-all high-tech solution might not be greeted with open arms by all. Scepticism abounds, especially by LFN who views such initiatives through the lens of civil liberties and potential state overreach. Our concerns – about privacy, surveillance, exclusion, and abuse of power – cannot be dismissed as mere paranoia; they serve as an important reminder that technology must be implemented in a way that *enhances* freedom and security for the people, not just for the state or corporate interests.

As we stand at this crossroads, the path forward should be guided by caution, inclusivity, and respect for choice. It would be wise for the government to proceed in a transparent, phased manner: build the digital ID infrastructure, but also build public trust

alongside it. Concrete steps like strengthening privacy laws, ensuring independent oversight, offering opt-out alternatives, and genuinely engaging with critics will determine whether this project becomes a celebrated success or a source of social conflict. Ideally, digital IDs in South Africa should become a tool that empowers citizens – for example, making life easier when dealing with bureaucracy or safeguarding one’s identity against theft – while rigorously guarding against any potential for misuse.

In closing, the debate around digital IDs might also open up a deeper dialogue about the kind of society we want to live in. Do we want a hyper-connected, fully tracked society if it promises safety and convenience? Or do we value a degree of anonymity and analogue living space as part of our freedom? Perhaps we can strike a balance: leveraging technology to improve lives without surrendering the fundamental rights and autonomy that many fought so hard to secure in our democracy. LFN and like-minded citizens remind us that vigilance is key – we must ensure that in embracing the future, we do not recreate the injustices of the past with new tools. The ultimate goal should be a South Africa where digital innovation and personal liberty go hand in hand, rather than one being sacrificed for the other.

Sources

1. Budeli, M. (2025). *Legal guardrails needed for smart ID roll-out in South Africa*. TechCentral. [8][11]
2. Macdonald, A. (2025). *South Africa introduces single digital ID as part of MyMzansi DPI plan*. Biometric Update. [2][3]
3. Burt, C. (2024). *South Africa begins work on national digital ID to stem fraud*. Biometric Update. [6][7]
4. Labuschagne, H. (2025). *Big questions about digital IDs in South Africa*. MyBroadband. [5][20]
5. Masthead (2020). *What is FICA?* (Financial Intelligence Centre Act overview). [12]

[1] [6] [7] [16] South Africa begins work on national digital ID to stem fraud | Biometric Update

<https://www.biometricupdate.com/202411/south-africa-begins-work-on-national-digital-id-to-stem-fraud>

[2] [3] [17] South Africa introduces single digital ID as part of MyMzansi DPI plan | Biometric Update

<https://www.biometricupdate.com/202510/south-africa-introduces-single-digital-id-as-part-of-mymzansi-dpi-plan>

[4] [5] [13] [14] [15] [19] [20] [21] [22] Big questions about digital IDs in South Africa – MyBroadband

<https://mybroadband.co.za/news/government/612552-big-questions-about-digital-ids-in-south-africa.html>

[8] [9] [10] [11] [18] Legal guardrails needed for smart ID roll-out in South Africa

<https://techcentral.co.za/legal-guardrails-needed-for-smart-id-roll-out-in-south-africa/272585/>

[12] Financial Intelligence Centre Act (FICA) - Masthead

<https://www.masthead.co.za/compliance/fica/>