LEGAL UPDATES 2025

YEAR IN REVIEW

Regulating Innovation: An Update on Telecommunications, Media & Technology Law in South Africa

PPM

ATTORNEYS

Information Security | Media | Technology | Infrastructure Projects

www.ppmattorneys.co.za

Table of contents

Introduction

As 2025 draws to a close, we at PPM Attorneys are reflecting on the key legal and regulatory shifts that have shaped the Technology, Media, and Telecommunications ("**TMT**") landscape over the past year. These updates highlight the key legal milestones of 2025 and outline what organisations should prepare for as we enter 2026.

Privacy and Information Security

POPIA GOT A DIGITAL MAKEOVER – Is your organisation going to evolve or fall behind?

In April, the Protection of Personal Information Act ("**POPIA**") underwent one of its most significant transformations yet. The 2025 amendments, published under Government Gazette Notice No. 6126, are bold, forward-thinking, and already in force. These revisions are not just legalese or red tape; they represent a shift in how organisations need to approach personal data.

The first major shift is a language update that reflects the times. The amended regulations introduce clearer, more contemporary definitions to words such as "complainant," "relevant bodies," and a modernised interpretation of "writing." Simply put, this means less ambiguity and greater inclusivity, particularly for those engaging with services digitally or from historically marginalised communities.

Say goodbye to mountains of paperwork and postage stamps! Under the new rules, data subjects can now object to data processing or request corrections through WhatsApp, SMS, email, or even in person, completely free of charge. Even requests made over the phone count, as long as they are properly recorded and accessible if needed.

The updated regulations put Information Officers squarely in the spotlight. Gone are the days when compliance could be treated as a once-off checklist exercise. Instead, organisations are now expected to take an active, ongoing role in strengthening and adapting their data protection practices. This shift recognises that compliance is not static; it's a living process that grows as technology, community needs, and regulatory expectations evolve. Think of it as compliance with momentum: always moving forward, always maturing, and always raising the bar.

Another significant shift that has been introduced is that "opt-out" consent is no longer sufficient. The threshold for valid consent has been raised. Consent is required to be explicit, informed, and properly recorded. Organisations wishing to market to individuals must now obtain clear permission, whether through email,

SMS, WhatsApp, fax, or even automated calls. This development closes the gap on questionable marketing practices and paves the way for more transparent, respectful, and trust-based engagement.

The complaints system has undergone a major upgrade. Complaints can now be lodged not only by individuals, but also by proxies, third parties, and public interest organisations, broadening access to justice. To further enhance inclusivity, the Information Regulator is required to provide assistance in languages beyond English, ensuring accessibility for diverse communities. The system is also backed by clear timelines, including a firm 14-day deadline for transferring complaints to the Regulator.

In the past, administrative fines had the potential to cripple smaller organisations. The updated regulations introduce a more flexible approach, allowing fines to be paid in instalments where an organisation's financial circumstances warrant it. This isn't about granting leniency to these organisations; it's about adopting a smarter, more sustainable model of enforcement that balances accountability with practicality.

The era of box-ticking compliance is over. Organisations must update policies, train staff, improve marketing practices, and enable real-time communication with data subjects. This is not just about avoiding fines, it's about building trust, protecting reputations, and gaining a competitive edge through strong data protection.

Privacy Behind the Gates: What the POPIA Code Means for Residential Communities

The Residential Communities Industry POPIA Code of Conduct ("**the Code**") sets out how personal information must be lawfully processed within South Africa's residential community sector. Developed by the Residential Communities Council ("**RCC**") and the National Association of Managing Agents ("**NAMA**"), the Code aligns with POPIA and provides practical guidance for estates, homeowners' associations, body corporates, and managing agents.

The Code's main goal is to ensure that all stakeholders in the residential community industry comply with POPIA. It promotes transparent information handling practices, consistent compliance frameworks for personal data

protection, and accountability through enforcement. RCC and NAMA have made compliance with the Code a condition of membership, ensuring that members actively apply its principles in practice.

The Code applies broadly to RCC and NAMA members, homeowners' associations, body corporates, managing agents, and related service providers. It covers the processing of data relating to homeowners, residents, visitors, employees, contractors, and suppliers. This wide scope reflects the reality that, from access control details to financial and contractual records, residential schemes process large amounts of sensitive information daily.

At the Code's heart are eight conditions for lawful processing, adapted from POPIA for the residential sector:

- **Accountability –** governing bodies and boards must take ultimate responsibility for compliance.
- **Processing Limitation –** personal information must be collected lawfully, only when necessary, and with consent where required.
- **Purpose Specification –** data may only be collected for clear, lawful purposes, such as levy collection, security, or service delivery.
- **Further Processing Limitation –** information cannot be reused for purposes unrelated to its original collection.
- **Information Quality –** records must be complete, accurate, and kept up to date.
- **Openness –** schemes must notify individuals when their data is collected and publish a PAIA Manual explaining processing practices.
- **Security Safeguards –** reasonable technical and organisational measures must be in place to protect data.
- **Data Subject Participation –** individuals must have the right to access, correct, or request deletion of their personal information.

The Code also recognises the heightened sensitivity of special categories of personal information such as biometric data, medical records, bank details, and the information of children. It requires responsible parties to conduct risk assessments and put in place proportionate protections before processing such

data. This is particularly important in residential communities where biometric systems and security records are increasingly common.

Each scheme must appoint an Information Officer, who is responsible for developing and maintaining a compliance framework. This officer oversees day-to-day processing practices, handles data subject requests and complaints, and reports annually to the Information Regulator. By centralising responsibility, the role ensures that every scheme has a clear point of accountability.

The RCC and NAMA monitor compliance with the Code through annual reporting and questionnaires. Complaints can be raised internally and, if unresolved, may be escalated to the Information Regulator. In some cases, an Independent Adjudicator may be appointed to resolve disputes, ensuring fairness and impartiality in the enforcement process.

In conclusion, the Residential Communities Industry POPIA Code of Conduct provides a structured and practical approach to managing personal information in residential schemes. By embedding accountability, transparency, and security safeguards, the Code not only ensures compliance with POPIA but also strengthens trust among residents, service providers, and governing bodies in South Africa's growing residential community sector.

Johannesburg's CCTV By-Law Repealed: POPIA Takes Centre Stage

The City of Johannesburg ("**CoJ**" or "**the City**") previously introduced a draft CCTV By-Law which sought to regulate the installation and operation of closed-circuit television ("**CCTV**") cameras. The draft required individuals and businesses to apply for the approval of, and register any cameras positioned to capture views of public spaces. Its stated purpose was to ensure lawful use, regulate registration, and assist in crime prevention.

The draft By-Law applied broadly to *"all CCTV camera and mobile camera, including drone camera, in Public Space; [or] in a private property with a view or angle of coverage to a Public Space, installed or intended as provided for, in the area and jurisdiction of the City."* It prohibited the installation or operation of such cameras without prior written approval from the City. Even modifications to an existing, approved system required new authorisation.

The proposed framework was met with strong resistance from civil society and business stakeholders. The Organisation Undoing Tax Abuse ("**OUTA**") and the South African Property Owners Association ("**SAPOA**") led objections, raising concerns that the By-Law was overreaching, unnecessary, and procedurally flawed. Specific criticisms centred on privacy infringements for property owners and the lack of meaningful public consultation.

Following legal challenges from OUTA and SAPOA, the By-Law has reportedly been repealed. OUTA has publicly welcomed the decision, while the City of Johannesburg has yet to release an official statement confirming the repeal.

The repeal creates a regulatory gap as there is currently no municipal framework specifically governing CCTV surveillance in Johannesburg. However, this does not mean businesses and private individuals are unregulated. POPIA provides the applicable framework as it seeks to promote the protection of personal information processed by both public and private bodies, establishing conditions for lawful processing.

For businesses, CCTV systems process personal information by capturing identifiable images of individuals. As such, POPIA compliance is mandatory. Examples of obligations include:

- **Transparency:** placing signage or notices to alert individuals that recording is taking place.
- **Retention:** keeping footage only for as long as reasonably necessary.
- **Access control:** restricting access to stored footage to protect data security.
- **Data subject rights:** providing copies of footage to individuals captured, upon lawful request.
- **Sharing restrictions:** limiting disclosure of footage to circumstances where a legal basis exists.

The repeal of the draft By-Law has been celebrated as a victory for privacy and regulatory certainty. Nonetheless, it raises important policy questions. To what extent should municipalities regulate private surveillance? How should authorities balance public safety with constitutional privacy rights? And should future regulations be integrated with POPIA rather than creating overlapping compliance obligations?

The use of CCTV cameras and their privacy implications was addressed in the Western Cape High Court matter of Phillips and Varkel v Bradbury, which provides some guidance in their use in the context of private parties. In Johannesburg, for now, businesses and residents must rely on POPIA as the primary legal framework when using CCTV, dashcams, or other surveillance tools. Compliance with POPIA's conditions is not optional; it remains essential to ensure lawful processing of personal information.

The Constitutional Court Draws the Line on Privacy and Online Expression

On 9 October 2024, the Constitutional Court delivered judgment in Botha v Smuts and Others. The case arose after Mr Smuts posted photographs of Mr Botha's animal trapping activities on Facebook, together with his name, farm address, and brokerage business details (which also revealed his home address). The Court held that publishing the farm location was permissible as it related to commercial operations and was in the public interest. However, it found that publishing Mr Botha's home address, even though it was also used for his business, unjustifiably infringed his privacy as it was peripheral to the public debate and posed serious risks to his and his family's safety. The Constitutional Court's reasoning provides important guidance on the treatment of personal information in the digital environment. The judgment makes clear that:

- **Voluntary disclosure reduces but does not extinguish privacy rights -** Publishing personal details online or on business websites may diminish an individual's expectation of privacy, but it does not amount to an open licence for all purposes.
- **Purpose matters -** Personal information shared for one purpose cannot automatically be used for another, especially when doing so intrudes into the private sphere.
- **Balancing rights is of utmost importance -** Courts will weigh privacy against freedom of expression. Disclosures that are not essential to public interest debates will not justify an invasion of privacy.
- **Relief may still be granted even after information has spread -** The Court signalled that mootness arguments carry less weight where ongoing harm results from the continued disclosure of private details.

Although the dispute pre-dated POPIA, the decision reinforces core POPIA principles, particularly around the lawful processing of personal information made public online. Businesses, media outlets, and individuals must recognise that sharing information from public sources or social media is not automatically permissible. The case highlights the importance of assessing both the purpose for which data was originally disclosed and the impact of reusing that information.

For practitioners, this judgment will serve as important precedent when advising clients on privacy disputes, online expression, and the intersection between constitutional rights and data protection.

Telecommunications

South Africa's telecoms and broadcasting sectors have had another year marked by regulatory shifts, policy debates and significant technological developments. From discussions around electronic communications services and call termination rates, to spectrum allocation and digital migration - the landscape has been filled with challenges and opportunities.

Digital Terrestrial Televisions Regulation After Migration

The Independent Communications Authority of South Africa ("**ICASA**") published Draft Digital Terrestrial Televisions Regulations for public comment. The Regulations indicate ICASA's desire to open up the broadcasting space to new entrants. Although the 'Invitation to Apply' process is very competitive, it will be refreshing to see new players in the broadcasting space.

Policy Direction: Individual ECNS Licences and Competition

A potentially progressive policy discussion has emerged around whether new Individual Electronic Communications Network Services ("**IECNS**") licences should be issued to improve competition and the universal provision of electronic communication services. The current regulatory framework only allows ICASA to consider applications for licence transfers, not new applications. This leaves barriers for entry quite high for new service providers to enter the scene.

If the proposed inquiry proceeds, we could see the opening-up of IECNS licensing, which would lower barriers to entry, lower prices of services, and improve service delivery in under-served/rural areas. We could see more investment in infrastructure, new access models, opportunities for hosts and rural internet service providers ("**ISPs**") and utility-backed networks. It will be interesting to see how ICASA approaches the competing market dynamics to change network access for the years to come.

Satellite-to-Mobile Trials & Emerging Services

The emergence of satellite-to-mobile services and new partnerships between

mobile operators and satellite companies provides an opportunity for expanding coverage to rural and underserved areas. This technology offers mobile connectivity where terrestrial infrastructure would be too costly or challenging to roll out. We can expect to see new approaches from both infrastructure-based providers and service resellers as they adapt to this growing space.

Transformation Reform: Extending Equity Equivalent Investment Programmes to Telecoms

The Minister of Communications and Digital Technologies released a Draft Policy Direction seeking to permit ownership of individual broadband network and services licences in South Africa without the current standard Electronic Communications Act B-BBEE requirements. Instead, the Policy Direction considers changing the licensing laws to include equity equivalent programmes to allow multinational companies alternative ways of entering the South African market (whilst having a positive impact on South Africa's economic development).

The conversation around transforming the ICT sector is still ongoing but we can expect to see tighter alignment between licensing and transformation obligations.

Call Termination Rates: Downward Path

Call termination rates remain a central issue in the telecoms landscape. In South Africa, high termination rates have created barriers for smaller operators who cannot compete effectively with incumbents on price. ICASA's ongoing review of these rates has been aimed at lowering costs and stimulating competition, though larger operators have certainly raised their frustrations, arguing that further reductions undermine their investment capacity.

With the lower rates gazetted in July 2025 and possible further reductions through 2027, consumers are certain to benefit.

Broadcasting & Digital Migration

South Africa has made progress toward digital migration, but repeated extensions of the analogue switch off date have frustrated stakeholders in the broadcasting sector. Each delay hampers the efficient use of valuable spectrum that could support broadband expansion, particularly in underserved areas. Hopefully,

government and industry will finally see the migration process come to a close so that we can see the full economic and social benefit this project promises.

Looking ahead, the coming years are likely to see more competition resulting from the reduced call termination rates, the satellite-to-mobile offerings will likely shift from pilot stages into commercial deployment – raising opportunities for partnerships and joint ventures with local operators. If we get to see the completion of the analogue switch-off project, then we could expect the release of spectrum, creating opportunities for more investment in 4G and 5G – particularly where mobile broadband is the most practical route for connectivity.

Media

The High Court confirms that citizens are allowed to record police officers without fear of arrest

In the judgment of Jacobs v Minister of Police and Others (2021/6576) [2025] ZAGPJHC 722, the Johannesburg High Court has confirmed that South African citizens have the right to film on-duty police officers. The judgment awarded an attorney, Mr Shaun Jacobs, R250,000.00 in damages, R150,000.00 for unlawful arrest, plus R100,000.00 for unwarranted detention. The case arose from an incident on 1 March 2019, when Jacobs encountered a roadblock set up directly in front of his home in Kempton Park. After being allowed to park inside his yard, Jacobs went inside his home to discuss the disruption caused by the roadblock with his wife. Shortly after, he approached the police officers to inquire whether they would be willing to relocate the roadblock to an unoccupied area nearby. When Jacobs calmly asked for the officers' details, one officer became aggressive, pushing Jacobs on the chest and demanding that he return to his house or face arrest.

Jacobs then went to retrieve his phone and began recording the scene. He contended that his intent was simply to capture footage of the roadblock to file a complaint with the appropriate authorities. However, when police officers saw him filming their conduct, they arrested him. The officers arrested Jacobs for crimen injuria, which is the act of unlawfully and intentionally impairing the dignity or privacy of another. In his lawsuit, Jacobs brought a defamation claim against this allegation, but Judge Twala dismissed the claim. However, Judge Twala emphasised that "citizens are entitled to ask questions and are entitled to explanations from law enforcement officers," as long as they do not interfere with police duties. For Jacobs, the award was both a personal vindication and just compensation for the unlawful arrest and ill-treatment during his 26-hour detention. It is also a reminder that citizens have the right to engage with police officers in a lawful manner, ask questions, and record police conduct without fear of arrest or punishment.

The Constitutional Court Restores RICA Functionality After Legislative Delay

On 25 July 2025, the Constitutional Court delivered a unanimous judgment, written by Deputy Chief Justice Madlanga, in response to an urgent application from the President of South Africa. The President had approached the Court directly, asking for temporary relief because certain sections of a key law, the Regulation of Interception of Communications and Provision of Communication-Related Information Act ("**RICA**"), had become unconstitutional and inoperable.

This issue traces back to a 2021 case brought by investigative journalists *AmaBhungane*, where the Court found parts of RICA to be unconstitutional. These problems included insufficient protection for journalists and lawyers, failure to properly inform people after they had been placed under surveillance, and the risk of abuse stemming from how judges were appointed to authorise surveillance.

The Court had given Parliament three years to fix the law and had put temporary measures in place to allow surveillance to continue legally during that period. In December 2023, just before the deadline, Parliament passed a new bill. Due to a variety of reasons, the President did not sign the bill into law before the deadline. He later realised, after being advised by his legal team, that the temporary measures had also expired. As a result, RICA was no longer functional, and no judge could lawfully authorise surveillance requests. This led to a backlog of unprocessed applications and posed a serious threat to national security, as intelligence and law enforcement agencies were left without legal tools to carry out surveillance.

The President asked the Court to step in and provide a temporary solution until Parliament finalised the necessary changes to RICA. He did not ask the Court to extend the original suspension period but instead requested new temporary measures to allow the law to function in the meantime.

The Court agreed that allowing RICA to remain inactive was not an option, given its importance in tackling serious crimes, protecting public safety, and maintaining national security. It decided to grant an updated set of temporary measures. This included authorising the Chief Justice to nominate three retired judges to serve as designated judges. These judges would be officially appointed by the Minister of Justice for fixed, non-renewable terms. This change addressed

previous concerns about the independence and reappointment of designated judges.

In addition to resolving the issue of judge appointments, the Court also reinstated two important protections:

- Where someone targeted for surveillance is a journalist or a lawyer, this must be disclosed in the application. The judge must be satisfied that the surveillance is truly necessary and must take steps to protect journalists' sources and clients' legal privilege.
- People who were placed under surveillance must be informed of this after the surveillance ends, unless doing so would put an investigation or national security at risk. In such cases, the notification can be delayed with judicial approval, but only for limited periods.

The Court decided not to grant additional relief requested by the President, finding that the interim measures already addressed the urgent issues. It also did not make any order regarding legal costs.

By acting to ensure that the country's surveillance system could continue to operate legally while Parliament works on finalising the new law, the Court ensured that law enforcement and intelligence services are not left without the legal tools they need, while still protecting important constitutional rights.

South Africa Forces Meta to Stop Child Pornography Online

In July 2025, the Digital Law Company ("**DLC**"), led by Emma Sadleir, filed an urgent application in the Gauteng High Court in Johannesburg. The case involved disturbing content on Meta owned platforms (Instagram and WhatsApp) that showed explicit sexual material involving South African schoolchildren. The posts also named children and their schools and made claims about their HIV status. DLC said the material was being shared anonymously but had severe consequences.

The court became involved after a threat by the person managing the accounts to publish more content. Families had already reported serious harm, including that two people had taken their own lives. DLC argued that without urgent intervention, more harm would follow.

The High Court, led by Judge Mudunwazi Makamu, ordered Meta to remove dozens of Instagram profiles and WhatsApp channels that were distributing the content. Meta was told to permanently disable the people behind those accounts so they could not create new ones. Meta was also ordered to hand over all identifying data it had about those behind the accounts.

After the order, DLC claimed that while Meta did remove some accounts, new ones kept appearing. This prompted DLC to threaten Meta with contempt of court. In parallel, Meta and DLC negotiated and eventually agreed on additional measures to strengthen the court's orders.

Among those additional measures:

- Meta agreed to disclose details (names, addresses, and IP addresses where available) about over 60 offending accounts.
- Meta agreed to permanently remove, as far as possible, the flagged accounts and channels reported by DLC.
- A two-year hotline was to be established between DLC and Meta to deal quickly with urgent child protection content, so future reports get attention more reliably.

The case marks a turning point as it is possibly the first time in South African courts that a global tech company has formally agreed to such wide-ranging remedial steps in respect of harmful content involving children.

How WhatsApp Chats Helped Prove Provisional Liquidation in Gerritsen v Blydskap

In the case of *Gerritsen Trading CC t/a Gerritsen Drilling SA v Blydskap Holdings (Pty) Ltd,* the court relied heavily on WhatsApp messages to decide whether a provisional liquidation order should be granted. Gerritsen Drilling had been contracted by Blydskap Holdings to drill three boreholes. While the first two were completed without issues, the third encountered water pressure problems, leading to delays. Despite this, Gerritsen invoiced Blydskap for the work done, but a large portion of the invoice remained unpaid.

What made this case stand out was how WhatsApp messages between the two parties were used as key evidence. In those messages, Blydskap's director

acknowledged the debt several times and made repeated promises to pay, making statements like "I will pay this month" or "as soon as my clients pay, I will settle." These were not vague or disputed comments; the court found them to be clear acknowledgments of debt.

The WhatsApp conversations helped the court conclude three important things:

- that the debt was admitted;
- that Blydskap did not have a genuine or valid defence to avoid payment; and
- that Blydskap was commercially insolvent - shown by its repeated delays and excuses for non-payment.

The court viewed these messages as a reliable reflection of what was really going on at the time, far more persuasive than the arguments later raised by Blydskap in court.

Based on this, the court found that all the legal requirements for provisional liquidation were satisfied. Gerritsen was a legitimate creditor as there was no realistic defence to the claim, and Blydskap could not meet its financial obligations. As a result, the court granted a provisional liquidation order, placing Blydskap's assets under the control of the Master of the High Court pending final proceedings.

This case highlights how digital communication, particularly WhatsApp messages, can play a powerful role in commercial litigation, especially when proving debt and insolvency.

Technology Law

The Global scramble to govern Artificial Intelligence

Artificial intelligence ("**AI**") is advancing at an unprecedented pace, prompting governments around the world to develop regulatory frameworks that balance innovation with ethical oversight. The European Union ("**EU**") is leading the charge with its landmark AI Act, the first comprehensive legal framework for AI. This legislation categorises AI systems based on risk levels:

- unacceptable risk systems, such as social scoring, are banned;
- high risk systems, like those used in healthcare or law enforcement, face strict compliance requirements;
- limited risk systems must meet certain transparency obligations; and
- minimal-risk systems are largely unregulated.

The EU's approach emphasises fairness, explainability, and human oversight, setting a global benchmark for responsible AI governance.

In the United States, AI regulation is more fragmented. While there is no unified federal law, several frameworks guide ethical AI development. The Federal Trade Commission has also issued warnings about algorithmic bias and deceptive AI practices. At the state level, laws like California's Consumer Privacy Act indirectly regulate AI through data protection. This patchwork approach reflects the U.S.'s emphasis on innovation and market-driven oversight.

China has adopted a more centralised and assertive stance. Its regulations focus on controlling generative AI, algorithmic recommendation systems, and cybersecurity. The government enforces strict compliance to ensure AI aligns with national security interests and social stability. China's regulatory model emphasises state control, ethical boundaries, and rapid deployment of AI technologies, positioning itself as a global leader in AI governance.

The United Kingdom has taken a "pro-innovation" approach, opting for sector-specific oversight rather than sweeping legislation. Regulatory bodies such as the Financial Conduct Authority and the Information Commissioner's Office have

issued AI specific guidelines. The UK also hosted the 2023 AI Safety Summit, which aimed to foster international cooperation on AI ethics and safety.

Canada, meanwhile, is developing the Artificial Intelligence and Data Act, which focuses on high-impact systems and aims to ensure fairness, transparency, and accountability in AI deployment.

India has yet to introduce a standalone AI law, but regulates AI through existing legislation such as the Digital Personal Data Protection Act and the Information Technology Act. The government's policy think tank, NITI Aayog, has released guidelines promoting ethical AI development, with a focus on inclusive growth and digital empowerment.

In South Africa, AI is currently governed through a combination of existing laws and emerging policy frameworks. While there is no dedicated AI legislation, laws such as the Protection of Personal Information Act, the Consumer Protection Act, and the Electronic Communications and Transactions Act address aspects of AI, particularly in relation to data privacy and automated decision-making. However, these laws leave gaps in areas like algorithmic bias, deepfakes, and AI-generated content. To address these challenges, South Africa introduced the National AI Policy Framework in 2024, spearheaded by the Department of Communications and Digital Technologies. This framework promotes ethical AI development, transparency, human-centred design, and sector-specific strategies in areas like healthcare and education. It also emphasises talent development and encourages collaboration between the public and private sectors. An AI Expert Advisory Council was established to guide the ethical, legal, and technical dimensions of AI regulation, with the goal of aligning South Africa's policies with global standards such as the EU AI Act. As of October 2025, the framework remains in draft form and has not yet been officially finalised. Public comments were invited until 29 November 2024, and the government has expressed its commitment to completing the framework to ensure responsible and inclusive AI governance.

South Africa is also actively engaging in global AI governance efforts. It participates in UNESCO's AI ethics initiatives and has used its G20 presidency to advocate for inclusive and equitable AI development. Legal experts in the country are calling for the creation of a Technology Law Commission to draft anticipatory legislation that can adapt to AI's rapid evolution. This would enable South Africa

to move from a reactive regulation to a dynamic, risk-based governance model that ensures both innovation and public trust.

National Data and Cloud Policy (2024)

The National Data and Cloud Policy aims to transform South Africa into a secure, inclusive digital economy by guiding how data is collected, stored, accessed, and used. I t emphasises the critical role of data in driving innovation, economic growth, and improved public services, while upholding high standards for privacy and security. Central to this vision is a cloud-first approach, where cloud services become the default option for new ICT procurement across all government departments and state entities.

Core Components

Cloud Service Models - The policy defines and promotes three key cloud service models:Software as a Service (SaaS): Applications delivered over the internet. Platform as a Service (PaaS): Tools and environments for developers.Infrastructure as a Service (IaaS): Virtualised computing resources.

Deployment Models - It outlines three deployment options to meet diverse organisational needs:

Private Cloud: Exclusive use by a single organisation.

Public Cloud: Services offered over the internet to multiple users.

Hybrid Cloud: A combination of private and public clouds for greater flexibility.

Strategic Goals

Data Sovereignty and Security - The policy underscores the importance of local data hosting and secure access, aiming to reduce dependence on foreign cloud providers and ensure compliance with South African laws. It also supports cross-border data transfer protocols that safeguard national interests.

Infrastructure and Investment - Acknowledging limited government resources, the policy promotes public-private partnerships to build and manage cloud infrastructure. It prioritises reliable energy supply, skills development, and system interoperability to attract investment and meet procurement demands.

Governance and Institutional Mechanisms

The State Information Technology Agency ("**SITA"**) is designated to source cloud services, develop service-level agreements, and establish technical standardsThis centralised. This centralised governance ensures consistency, transparency, and accountability across government departments.

Impact and Reception

The policy has been well received for its pragmatic shift from a centralised, government-owned data centre model to a decentralised, private-sector-driven approach. This transition enhances scalability, reliability, and cost-efficiency, while aligning South Africa with global best practices in cloud adoption and digital transformation.

The National Identity System

The National Identity System ("**NIS**") is a new, integrated platform being developed by the Department of Home Affairs to replace the outdated National Population Register. Expected to be fully operational by 2029, the NIS will serve as a single source of truth for all South Africans and legally recognised foreign nationals. It combines biographic data (name, birth date, ID number) and biometric data (fingerprints, facial images) into one secure, digital system.

Key Features include:

- Digitised registration of births, marriages, and deaths
- Centralised adjudication of permits and visas
- Integration with e-government and e-commerce platforms
- Enhanced fraud prevention and identity verification
- Use of e-gates at ports of entry for frequent travellers

The NIS is part of a broader 10-year modernisation program running through 2028/29, aimed at eliminating inefficiencies like long queues and identity fraud.

Conclusion

Here's a quick summary of the key legal and regulatory developments in the TMT sector in 2025.

Privacy and Information Security

The 2025 POPIA amendments raised the bar. Consent must be crystal clear! Information Officers are in the hot seat, and compliance is no longer a box-ticking exercise, but a living, breathing process. Those who keep up will build trust; those who don't will quickly fall behind.

The Residential Communities Code shows how privacy is moving into everyday spaces. From biometric gates to levy collections - estates, and HOAs now carry serious accountability for data handling.

With Johannesburg's CCTV By-Law scrapped, POPIA is firmly in charge. Businesses running cameras, dashcams, or drones must meet their rules, signage, retention limits, and data subject rights are all non-negotiable.

The Constitutional Court has drawn a clear line: public information online doesn't give everyone a free pass to share it. Context, purpose, and respect for privacy still matter.

2025 confirmed that privacy compliance can no longer be treated as an optional add-on, it is a non-negotiable obligation!

Telecommunications

This year saw telecoms shaped by regulatory debate, pricing battles, and new technologies. From spectrum delays to call termination rate cuts, the sector is under constant pressure to adapt.

ICASA's moves on Digital Terrestrial Television and ECNS licensing hint at more competition and lower barriers to entry, while satellite-to-mobile trials show real promise for rural coverage.

Transformation and equity-equivalent programmes remain on the agenda, as

does the long-delayed digital migration — the key to unlocking spectrum for 4G and 5G expansion.

In short, the sector is at a turning point. How quickly regulators and industry resolve these issues will determine whether South Africa's connectivity challenges become opportunities.

Media Law

2025 was a big year for media and digital rights. Courts affirmed that citizens could record police officers without fear of arrest, reinforcing accountability and transparency in law enforcement.

At the constitutional level, the RICA judgment restored critical surveillance safeguards while balancing national security with protections for journalists, lawyers, and ordinary citizens.

The urgent action against Meta marked a watershed moment in online safety, with a global tech giant compelled to take sweeping steps to remove child exploitation content and cooperate directly with local watchdogs.

Finally, the Gerritsen case showed how digital evidence, even WhatsApp chats, are reshaping commercial litigation, proving debts and insolvency with a level of clarity that traditional arguments often lack.

Together, these developments show how South African courts are grappling with the realities of digital society where privacy, safety, accountability, and technology intersect daily. The trend is clear: the law is catching up, and digital rights and responsibilities are firmly on the judicial agenda.

Technology Law

Technology law in 2025 reflects a global and local race to keep pace with innovation. From AI regulation to cloud policy, identity systems, and cybercrime enforcement, lawmakers are trying to balance opportunity with accountability.

South Africa's National AI Policy Framework, Data and Cloud Policy, and modernized identity systems show a clear shift towards digital-first governance, with privacy, security, and efficiency at the core.

In short, technology law is moving to the centre of South Africa's legal framework. It's fast, adaptive, and unavoidable!

That concludes our brief overview of the legal and regulatory developments in the TMT sector. Keep an eye on our social media pages for more updates in the new year.

About us

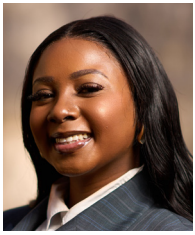
Lucien Pierce
Director

Lucinda Botes
Senior Associate

Tshegofatso Phahlamohlaka
Associate

Tshimangadzo Nengovhela
Candidate Legal Practitioner

Kgomotso Mabena
Candidate Legal Practitioner



Nokwanga Mkhize
Legal Intern

Luyanda Maema
Legal Intern

Palmer Katiyo
Office Administrator

Who we are

We are a **boutique commercial law firm** operating for over 21 years and focusing on corporate, commercial, regulatory and compliance aspects of information and communications technology (**ICT**) and related infrastructure, as well as data protection, and media law. We are 100% black owned and rated **Level 1 for BEE** purposes; an important factor when doing business in South Africa. We actively and passionately promote women empowerment. Our professional staff complement is typically about **90% women**. We have 12 client-focused principles that govern the way we operate. The firm has **7 professionals** and **1 administrative** staff member. The firm's professionals have over 70 years combined postadmission experience.

Our rates are **competitive**, and we have fee arrangements that suit different types of clients. Our clients benefit from a firm which is not the cheapest but also not ridiculously expensive. We offer value for money, without compromising standards. We save you money and the environment by operating an almost paperless office. We have firmly embedded processes that rely on electronic systems to ensure proper workflows and reporting to clients.

We all know that having a good lawyer on your team is crucial to long term success in business. Because of this, we would like to see ourselves as not only your lawyers, but your long-term partner. We have outstanding credentials and an unblemished track record, with a long list of great references. We focus on advising both state and private clients on achieving their strategic and commercial objectives through good, clear, precise legal advice and strategic support.

What we do

Information Security and Data Protection Law

Our firm has recognised experience in all aspects of information security regulations and international and South African data protection laws (POPIA, GDPR). We have been involved with POPIA since it was a discussion paper in 2003. Our submissions were considered in the SA Law Reform Commission's Privacy and Data Protection Report, 2009. We have been involved in and at the forefront of developments on this area of the law for 16 years. We have a team made up of legal and technology experts. We have advised multi-nationals, listed companies, state-owned entities and small to medium enterprises on POPIA and relate information security matters. We can assist you with all aspects of your privacy or information security compliance projects.

Technology, Information and Communications

From broadcasting licences to spectrum to ICT infrastructure, we are experts on the legislation and regulations surrounding this rapidly developing area of the law. Our services include advising on the licensing and regulation of the electronic communications networks and services.

Intellectual Property and Commercial Law

Our firm has considerable expertise in this area, particularly from an international perspective, from both contractual and regulatory standpoints. Our practice covers all types of private contracts and public law as well as due diligence exercises.

Media and Advertising Law

Our well researched opinions extend to both national and international laws on digital content, broadcasting, promotional competitions, and social media advertising.

Infrastructure Projects

We regularly advise on Public Private Partnerships. We have also built a solid knowledge database by advising multinational companies on construction and maintenance of communications infrastructure such as data centres and fibre optic networks.

PPM

ATTORNEYS

Information Security | Media | Technology | Infrastructure Projects

www.ppmattorneys.co.za