JUTA
POPIA PORTAL

ISSUE NO 73 • IS PRIVACY BECOMING A PAID FEATURE? • SEPTEMBER 2026

IS PRIVACY BECOMING A PAID FEATURE?

1. INTRODUCTION

There is a familiar bargain behind many digital services: the service appears to be free, but the user pays with personal information. Pay-or-consent models make that bargain explicit. The user is asked either to pay a subscription fee to avoid certain data processing, usually behavioural advertising, or to consent to that processing to access the service without paying.

At first glance this looks like a choice. But the question is whether it is a meaningful choice. If a user cannot afford the paid option, cannot realistically leave the platform, or depends on the service for social, professional or economic participation, consent may NOT be voluntary.

In her article *Privacy for Sale? The Legality of the Pay-or-Consent Model in South Africa, Zinhle Novazi* argues that the model exposes a serious gap in South African law: POPIA contains important consent principles, but it does not yet explain clearly how dominance, lock-in, digital dependency and inequality affect voluntariness. The risk is that privacy becomes a premium feature available only to those who can afford it.


Photo: iStock

2. UNDERSTANDING PAY-OR-CONSENT MODELS

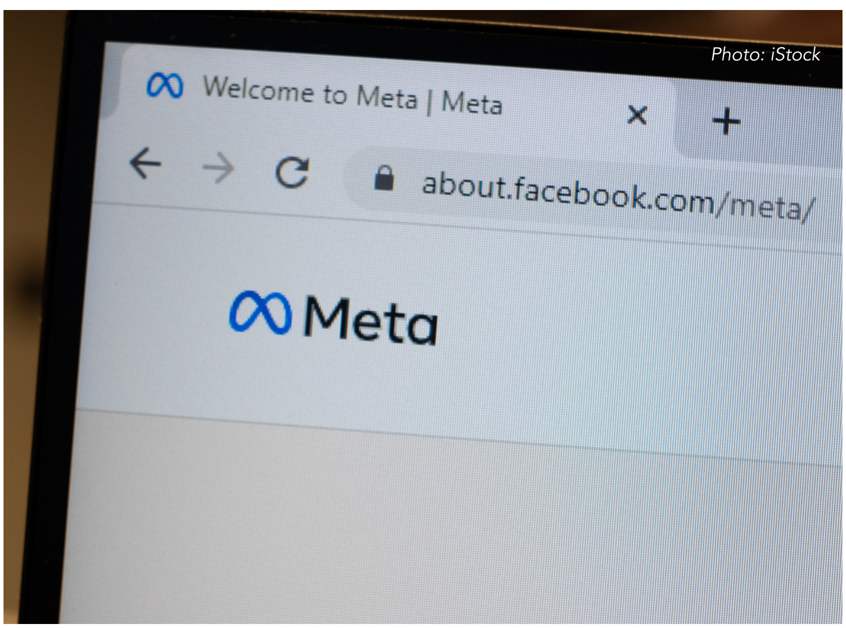

Photo: iStock

The pay-or-consent model, also called pay-or-okay, gives users two options: agree to data processing for behavioural advertising (or any other type of further or non-essential processing), or pay for a version of the service without that advertising or processing. One example is Meta's European subscription model for Facebook and Instagram, which prompted regulatory scrutiny under both data protection and digital markets law.

The model matters because behavioural advertising is not ordinary service delivery. It usually involves tracking users over time, combining data from different sources, profiling behaviour, inferring interests or characteristics, and using those profiles to target advertisements. That processing may be valuable to the platform, but value to the platform is not the same as being necessary for the user-facing service.

3. THE EU APPROACH: CONSENT MUST BE REAL, NOT THEORETICAL

Photo: iStock

The EU position is useful for South Africa because it provides a developed framework for consent in platform markets. In ***Meta Platforms v Bundeskartellamt***, the Court of Justice of the European Union confirmed that market dominance does not automatically invalidate consent, but it must be considered when assessing whether consent was freely given. The court also interpreted contractual necessity strictly: processing is not necessary merely because it improves monetisation or personalisation. It must be objectively necessary for the service.

The **European Data Protection Board's Opinion 08/2024** goes further. It states that, in most cases, large online platforms will not meet the standard for valid consent if they offer only a binary choice between consenting to behavioural advertising or paying a fee. A free alternative that does not involve behavioural advertising is an important factor in assessing whether users have a real choice.

The European Commission has also treated Meta's pay-or-consent model as a Digital Markets Act problem. In April 2025, it found that **Meta breached the DMA obligation** to give users a choice of a service using less personal data. Although South Africa does not have an equivalent to the DMA, the development shows how privacy, consumer protection and competition concerns converge in digital markets.

4. ASSESSING PAY-OR-CONSENT MODELS IN SOUTH AFRICA


Photo: iStock

POPIA defines consent as a voluntary, specific and informed expression of will. That definition should not be reduced to a tick box. In a pay-or-consent model, the responsible party should be able to show that the user had a fair and realistic ability to refuse.

Four POPIA questions follow.

- Voluntary: What happens if the user refuses? If refusal means exclusion from a socially or economically important service, or if the paid option is unaffordable, the consent is vulnerable.
- Specific: Is consent separated by purpose, or is one broad acceptance used for account creation, advertising, profiling, analytics, third-party sharing and service improvement? Bundled consent is risky.
- Informed: Does the user understand what personal information is collected, what tracking occurs, which partners receive the information, whether inferences are made, and how refusal or withdrawal works? Vague references to improving the user experience are not enough for invasive profiling.
- Proportionate: Even where consent is present, does the processing still comply with POPIA's minimality, purpose specification, openness, security safeguards, and data subject participation requirements?

The key point is that consent is not a cure-all. A responsible party cannot use consent to legitimise processing that is excessive, opaque, unfair or unrelated to a clearly defined purpose.

POPIA's minimality principle is central to any POPIA compliance assessment. Section 10 requires personal information to be adequate, relevant and not excessive for the purpose for which it is processed. A platform may need some information to create an account, secure access, and deliver the core service. It does not necessarily follow that extensive cross-site tracking, behavioural profiling or data enrichment is necessary for that service.

Responsible parties should therefore separate core service processing from optional commercial processing. The legal basis for account administration may differ from the legal basis for behavioural advertising. Treating all processing as one indivisible package undermines purpose specification and weakens consent.

5. DON'T FORGET CPA AND COMPETITION RISK

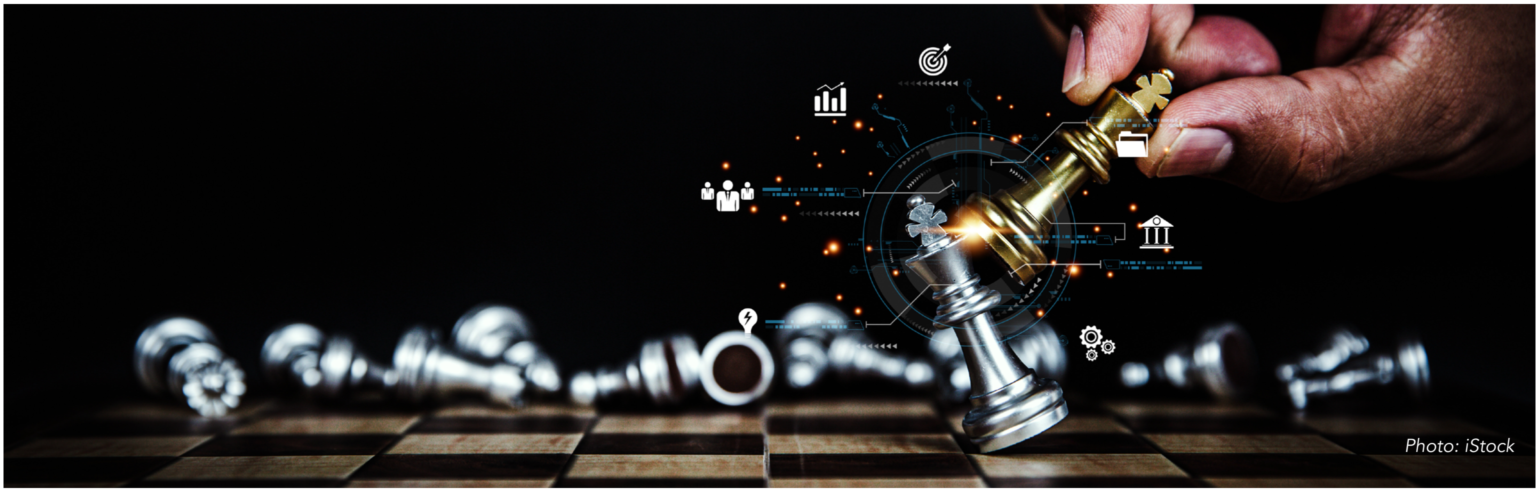

Photo: iStock

Novazi's article also considers consumer protection, contract and competition law. The Consumer Protection Act may be relevant because the user may be providing value even where no money changes hands. Personal information can function as a form of counter-performance. Sections 40, 48 and 52 of the CPA create possible routes to challenge coercive, unfair, unreasonable, unjust or excessively one-sided terms. A model that effectively says 'pay for privacy or surrender your data' may require closer scrutiny where consumers are financially vulnerable or where the service is difficult to avoid.

Competition law may also become relevant where a dominant platform uses its market power to impose unfair trading conditions or extract disproportionate value from users. The Competition Commission's digital market inquiries show growing regulatory attention to platform power in South Africa. The pay-or-consent debate therefore sits at the intersection of data protection, consumer fairness and competition policy.

6. PRACTICAL CONSIDERATIONS FOR RESPONSIBLE PARTIES

Photo: iStock

Responsible parties should not wait for a South African test case before reviewing consent-based monetisation models. POPIA requires responsible parties to perform personal information impact assessments on all processing activities. A practical assessment should cover the following.

- **Map the processing**. Identify what data is collected, inferred, shared, retained or used for profiling, advertising, or analytics.
- **Separate purposes.** Distinguish necessary service processing from optional advertising, personalisation, enrichment, analytics, or third-party sharing.
- **Test whether consent is truly voluntary.** Ask whether users can realistically refuse, whether the paid option is affordable and functionally equivalent, and whether refusal causes material detriment. Ensure that users may withdraw consent at any time without losing access to the service.

- **Make consent granular.** Allow users to accept or reject distinct processing purposes separately.
- **Use less intrusive alternatives.** Consider contextual advertising, limited personalisation, privacy-preserving analytics or a free version that does not require behavioural advertising.
- **Check direct marketing implications.** Consent to use a platform is not automatically consent to receive direct marketing from the platform, advertisers, or partners.
- **Review CPA and competition risk.** Consider whether the model could be viewed as coercive, unfair, one-sided, exploitative, or problematic in a market-power context.
- **Document the decision.** Record the assessment, the alternatives considered, the pricing rationale, the safeguards, the user information provided, and the review cycle.

7. CONCLUSION

Photo: iStock

Pay-or-consent models force an uncomfortable question out into the open: is privacy becoming something users must pay for?

POPIA does not prohibit data-funded digital services. It also does not require every online service to be free. But it does require personal information to be processed lawfully, minimally, transparently and for a defined purpose. It requires consent to be voluntary, specific and informed. And it requires responsible parties to account for the conditions under which that consent is obtained.

The practical lesson is that responsible parties should not treat consent as a shortcut. In digital markets, the test is whether users are given a fair, understandable and realistic choice.

8. FURTHER READING

Photo: iStock

- Zinhle Novazi 'Privacy for sale? The legality of the pay-or-consent model in South Africa' (2025) 3 *Stellenbosch Law Review*
- **Court of Justice of the European Union, Meta v Bundeskartellamt, Case C-252/21, 4 July 2023.**
- **European Data Protection Board, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, 17 April 2024.**
- **European Commission, 'Commission finds Apple and Meta in breach of the Digital Markets Act', 22 April 2025.**
- **Competition Commission of South Africa 'Online Intermediation Platforms Market Inquiry: Final Report and Decision', July 2023.**

juta