JUTA
POPIA PORTAL

ISSUE NO 74 • DATA PRIVACY ROUNDUP 2026 Q4 • NOVEMBER 2026

DATA PRIVACY ROUNDUP 2026 Q4

1. OVERVIEW

Recent developments reflect continued regulatory focus on enforcement, platform accountability, and technology-enabled surveillance. In South Africa, the Information Regulator is considering amendments to POPIA's enforcement regime and has begun proactively monitoring compliance. In the US, a multistate settlement with Meta addresses children's privacy and platform design, while the US Supreme Court has considered whether access to location information through a geofence warrant constitutes a search under the Fourth Amendment.



2. SOUTH AFRICA: WHAT COMES NEXT FOR POPIA?


Photo: iStock

At a media briefing on 31 August 2026, the Information Regulator outlined several areas of current regulatory focus.

It has received more than 8 000 security compromise notifications since POPIA became enforceable, including more than 1 220 since 1 April 2026, and expects more than 3 000 during the current financial year.

The Regulator also indicated that it intends to propose amendments to POPIA's enforcement regime. Under section 95, the Regulator may, after considering a recommendation of the Enforcement Committee, issue an enforcement notice requiring specified remedial steps or the cessation of specified processing. Failure to comply with an enforcement notice is an offence under section 103. Section 109 permits the Regulator to issue an infringement notice and impose an administrative fine, currently capped at R10 million, where a responsible party is alleged to have committed an offence under POPIA.

The Regulator regards this remedial period as a potential weakness because compliance with an enforcement notice may prevent the matter progressing to the offence and administrative-fine stage. It is considering updating POPIA to make provision for a model that would permit a fine once non-compliance has been established. No amendment has yet been made.

The Regulator has also begun proactively contacting responsible parties and requiring them to demonstrate compliance. This signals a move towards more active supervision and places greater emphasis on documented, demonstrable compliance.



Photo: iStock

3. META'S $17.1 BILLION SETTLEMENT

In August 2026, Meta agreed to a proposed settlement of up to 17.1 billion US dollars with US states and territories over claims concerning Facebook and Instagram. The settlement remains subject to court approval and Meta did not admit wrongdoing.

The litigation centred on allegations that Meta designed its platforms to encourage compulsive use by children and teenagers, and misrepresented their safety. The claims included alleged contraventions of the Children's Online Privacy Protection Act (COPPA) and state consumer protection laws.

COPPA applies to operators of online services directed to children and to operators with actual knowledge that they are collecting personal information from children under 13, and requires parental notice and verifiable parental consent. The states alleged that Meta had actual knowledge that children under 13 used Instagram and Facebook but continued to collect their personal information without the required parental consent. The federal complaint also alleged that Instagram, or parts of it, was directed towards children.

The information allegedly collected included geolocation information, persistent and device identifiers, photos, and videos. The issue was therefore whether Meta's knowledge of under-13 users triggered statutory obligations despite its stated age restriction.

The settlement also resolves separate state claims arising from Meta's historical sharing of Facebook users' non-public information with third parties, including conduct associated with Cambridge Analytica. Meta must pay approximately 459.3 million US dollars to participating states in respect of those claims. In return, the states release Meta from claims arising from the acts and practices alleged in their Cambridge Analytica complaints.

4. LOCATION DATA AND GEOFENCE WARRANTS



Photo: iStock

The US Supreme Court considered the privacy implications of geofence warrants in *Chatrie v United States*.

The case concerned a 2019 bank robbery in Virginia. Investigators obtained a warrant requiring Google to provide location history data for devices within a 150-metre radius of the bank around the time of the robbery. Google first produced anonymised location data; investigators narrowed the group and obtained additional location information; and Google then disclosed identifying information for the remaining users. The process identified Okello Chatrie.

On 29 June 2026, the Supreme Court held that government access to Chatrie's location history constituted a 'search' under the Fourth Amendment. Applying *Carpenter v United States*, the court held that a person has a reasonable expectation of privacy in this form of location information because it enables detailed retrospective reconstruction of a person's movements.

The court also rejected the government's reliance on the third-party doctrine, under which voluntarily disclosed information will generally attract a reduced expectation of privacy. *Carpenter* had declined to apply that doctrine to cell-site location information because of its revealing nature and because it is not meaningfully 'shared' in the ordinary sense. The court held that the same reasoning applied to Google Location History, despite the information being stored by a technology provider.

Importantly, the court did not decide that the geofence warrant itself was unlawful. It remitted the matter to the Court of Appeals to determine whether each stage of the warrant satisfied the Fourth Amendment requirements of probable cause and particularity. The judgment establishes that accessing location history is a search, while the validity of a particular warrant still depends on its scope and justification.

Although *Chatrie* was decided under US constitutional law and does not determine the application of POPIA, it illustrates the sensitivity of location information and the privacy implications of datasets that allow a person's movements to be reconstructed retrospectively.

5. CONCLUSION


Photo: iStock

These developments show regulators and courts focusing increasingly on the substance of data-processing practices. The Information Regulator is considering a more direct enforcement model; the Meta settlement demonstrates how children's privacy can intersect with product design and consumer protection law; and *Chatrie* confirms that highly revealing information may retain constitutional protection even when held by a technology provider.

For legal and compliance teams, the common requirement is to understand not only what personal information is processed, but why and how it is processed, what risks arise from the technology used, and whether compliance can be demonstrated if challenged.

6. READ MORE



- Information Regulator *The Information Regulator briefs members of the media on key POPIA and PAIA matters, 31 August 2026*, **Information Regulator media briefing**.
- California Department of Justice *Attorney General Bonta Secures Transformative $17 Billion Settlement with Meta, Proposed Settlement Includes Fundamental Changes to Instagram and Facebook, 26 August 2026*, **California Attorney General announcement**.
- *People of the State of California et al v Meta Platforms Inc et al* Case No 4:23-cv-05448-YGR, proposed settlement agreement, 26 August 2026, **Meta settlement materials**.
- California Department of Justice *Attorney General Bonta Files Lawsuit Against Meta Over Harms to Youth Mental Health*, 24 October 2023, (including the federal multistate complaint alleging contraventions of COPPA and state consumer protection laws), **Meta multistate litigation and complaint**.
- *Chatrie v United States*, 609 US ___ (2026), No 25-112, judgment of the US Supreme Court, 29 June 2026, **US Supreme Court judgment in Chatrie**.
- **Chapter 5:** Information security management.
- **Chapter 19:** Enforcement of POPIA.

juta

© Juta and Company (Pty) Ltd. All rights reserved.