Youth Justice (Electronic Monitoring) Amendment Bill 2025

Submission No: 023
Submission By: Office of the Information Commissioner
Publication: Making the submission and your name public

12 January 2026

Mr Nigel Hutton
Chair
Education, Arts and Communities Committee
Queensland Parliament

By email: eacc@parliament.qld.gov.au

Dear Chair

Inquiry into the *Youth Justice (Electronic Monitoring) Amendment Bill 2025*

The Office of the Information Commissioner (**OIC**) welcomes the opportunity to make a submission to the Education, Arts and Communities Committee's inquiry into the *Youth Justice (Electronic Monitoring) Amendment Bill 2025* (**Bill**).

In 2021, the *Youth Justice Act 1992* (**YJ Act**) was amended to facilitate an electronic monitoring trial as a condition of bail for eligible offenders. The trial progressively expanded in duration and scope, with an evaluation report (**Report**) tabled in Queensland Parliament in December 2025.[1] The Report found that electronic monitoring devices appear to be complementing other supports to achieve positive outcomes including high bail completion, reduced reoffending, lower victimisation and less time in custody.[2]

The Bill proposes to amend the YJ Act and *Youth Justice Regulation 2016* to make the imposition of electronic monitoring bail conditions permanent and statewide, to remove current eligibility criteria and to simplify matters considered by the court.

OIC notes there are inherent privacy risks associated with the surveillance and recording of a person's movements and whereabouts through an electronic monitoring device. However, an individual's right to privacy is not absolute[3] and an appropriate balance must be struck with other competing rights, including community safety and the implementation of an order or decision made by a court.

OIC's comments focus on privacy impacts, information sharing as well as facilitating the public's right to access government-held information.

About the OIC

OIC is an independent statutory body that reports to the Queensland Parliament. The Information Commissioner is an Officer of Parliament and is charged with functions under the *Right to Information Act 2009* (**RTI Act**) and the *Information Privacy Act 2009* (**IP Act**).

[1] Evaluation of the Electronic Monitoring Trial: Final Report (October 2025) prepared by the Department of Youth Justice and Victim Support.
[2] Report at p6.
[3] Section 13 of *Human Rights Act 2019*.

The RTI Act promotes openness, accountability and transparency by facilitating greater access to government-held information. It promotes the administrative release of government-held information as a matter of course, with formal access applications under the RTI Act being necessary only as a last resort.

The IP Act provides safeguards for the handling of personal information in the public sector environment. It sets out the Queensland Privacy Principles (**QPPs**) which govern the collection, management, use and disclosure of personal information by Queensland public sector agencies. An agency will not necessarily breach privacy principles relating to disclosure of personal information where disclosure is required or permitted under another Act.

Privacy impacts

Consistent with 'privacy by design' methodology, it is recommended that a comprehensive Privacy Impact Assessment (**PIA**) is conducted due to the nature of the amendments proposed.[4]

OIC notes that activities within the trial are delivered collaboratively by Department of Youth Justice and Victim Support (**YJVS**), Queensland Police Service (**QPS**) and Queensland Corrective Services (**QCS**). The operational burden is carried largely by QCS through monitoring and QPS and Youth Co-Responder Teams (**YCRTs**) through supervision and response.[5]

The PIA should identify privacy impacts, assess compliance with the QPPs, develop mitigating measures and formulate a privacy risk management approach. Specifically, all relevant government agencies (namely YJVS, QPS and QCS) and non-government agencies (contracted service providers)[6] will need to be identified to ensure the handling of personal and sensitive information complies with the QPPs (unless an exemption applies) and is authorised by law. Subject to the special provision for a 'law enforcement agency'[7] in section 29 of the IP Act, the QPPs of particular relevance include:

- open and transparent management of personal information (QPP 1)
- collection of personal[8] and sensitive[9] information (QPP 3)
- use and disclosure of personal and sensitive information (QPP 6)
- ensuring the quality of the personal information (QPP 10)
- protecting the information from misuse, interference and loss, and from unauthorised access, modification and disclosure (QPP 11.1), and
- destroying information no longer needed or ensuring the information is de-identified (QPP 11.2).

[4] Note: If a PIA has been conducted previously, it is recommended it be updated.
[5] Report at p7. Note: YCRTs comprise YJVS and QPS staff.
[6] See sections 35-36 of IP Act relating to contracted service providers, noting the Report refers to outsourced service delivery and bail support staff (NGO) at p39.
[7] 'Law enforcement agency' is defined in schedule 5 of the IP Act and includes QPS, QCS and 'any other agency, to the extent it has responsibility for … the performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed', or '… the execution or implementation of an order or decision made by a court or tribunal'.
[8] 'Personal information' is any information about an identifiable, or reasonably identifiable, individual (see section 12 of IP Act).
[9] 'Sensitive information' is a subset of 'personal information' and includes information about a criminal record (see schedule 5 of IP Act). It attracts a higher level of protection under the QPPs.

The retention period for personal information should be given careful consideration and tailored for specific purposes, or as a general rule limited to a strict minimum. In many surveillance cases, personal information need only be retained for a short period. A report by the Australian Human Rights Commission found that in 80% of cases, telecommunications data requested by law enforcement agencies was less than three months old.[10] By giving the retention period careful consideration, the agency can address the significant privacy concerns relating to long-term surveillance without impacting on the purposes of the data collection. The potential risk of interfering with an individual's personal privacy can be significantly reduced by securely destroying the personal information as soon as it is no longer necessary for a specified purpose. The longer the information is retained, the greater the window of potential harm from loss or misuse.

Information sharing

The Report details operational challenges encountered during the trial and provides that, 'Although the multi-agency working group developed detailed guidelines and information-sharing protocols, including workflow charts for QPS and YCRT outlining roles and suggested actions, stakeholders still reported confusion around responsibilities and how alerts should be actioned.'[11]

The Report set out future considerations relating to operational improvements and shared inter-agency arrangements. In relation to the latter, it provides:

> While existing legal frameworks provide a foundation for coordination, the absence of a robust shared system has limited consistent and timely data sharing and evaluation across partners. Reviewing and updating the MoU for this trial would help formalise protocols and strengthen collaboration. Additional frameworks or systems may also be needed to support robust monitoring, adaptive delivery, and informed EM policy decisions.[12]

OIC refers to the recent amendments to the *Domestic and Family Violence Protection Act 2012* (**DFVP Act**) and *Domestic and Family Violence Protection Regulation 2023* (**DFVP Regulation**) relating to the imposition of a monitoring device condition when making a domestic violence order as part of a two-year pilot.[13] Of relevance is the new information sharing framework inserted in the DFVP Regulation for information relating to the monitoring device condition, which includes permitted uses, limitations, recording and storing.[14] As stated in the Explanatory Notes, whilst an existing information sharing framework is contained in Part 5A of the DFVP Act, it does not sufficiently capture the information sharing required for the pilot.[15] OIC also notes a new criminal offence provision is inserted in the DFVP Act for the misuse of monitoring device information.[16]

---

[10] *Review of the mandatory data retention regime*: Australian Human Rights Commission submission to the Parliamentary Joint Committee on Intelligence and Security (July 2019) at p10.
[11] Report at p7-8.
[12] Report at p10.
[13] *Domestic and Family Violence Protection and Other Legislation Amendment Act 2025* and *Domestic and Family Violence Protection and Other Legislation Amendment Regulation 2025.*
[14] Part 2, Division 2 of *Domestic and Family Violence Protection Regulation 2023*; section 66F(1) of *Domestic and Family Violence Protection Act 2012*.
[15] Explanatory Notes*: Domestic and Family Violence Protection and Other Legislation Amendment Regulation 2025* at p5.
[16] Section 66F(2) of DFVP Act.

Similarly, an information sharing framework is contained in Part 9, Division 2A of the YJ Act. OIC submits that consideration should be given to including an information sharing framework specific to the electronic monitoring device condition in the youth justice legislation (potentially extending to offence provisions as well). This would assist with providing clarity and reducing the issues referred to in the Report.

Information access

As the trial transitions to permanency, it is recommended that a 'Transparency by Design' approach is adopted in relation to the information generated through the technology-based electronic monitoring mechanism.

This approach requires agencies to proactively consider and address how information and data gathered through technology enabled law enforcement arrangements meets relevant privacy and right to information obligations. From an access to information perspective, clarity about which of the relevant agencies holds information, and how such information can be accessed, is relevant where access to the information is requested under the RTI Act, and is also relevant to ensuring the relevant agency's accountability under the QPPs.

Thank you for the opportunity to make a submission. We trust our comments will assist the Committee in its work. Should you require further information, please contact us at [redacted] or on [redacted].

Yours sincerely

[redacted]

Joanne Kummrow
Information Commissioner