Corrective Services (Emerging Technologies and Security) and Other Legislation Amendment Bill 2022

Submission No: 2

Submitted by: Office of the Information Commissioner

Publication:

Attachments:

Submitter Comments:

Office of the Information Commissioner
Queensland

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

12 December 2022

Committee Secretary
Education, Employment and Training Committee
Parliament House
George Street
Brisbane Qld 4000

By email only: eetc@parliament.qld.gov.au

Dear Secretary

Inquiry into Corrective Services (Emerging Technologies and Security) and Other Legislation Amendment Bill 2022

We refer to the above inquiry.

The purpose of this letter is to convey the Office of the Information Commissioner's (**OIC**) submissions on aspects of the *Corrective Services (Emerging Technologies and Security) and Other Legislation Amendment Bill 2022* (**the Bill**), for the Committee's consideration.

OIC's submissions focus on the following amendments to the *Corrective Services Act 2006* (**CSA**) as proposed in the Bill:

- Clauses 16-20 and 36 of the Bill, intended to provide clear authority for the use of x-ray body scanners, body-worn cameras (**BWCs**) and other emerging technologies within corrective service facilities, to maintain safety and monitor threats; and
- Clauses 31-32, which propose to enhance information sharing powers, to promote prisoner health and wellbeing, support frontline service delivery and interagency collaboration.

We have also identified a definitional issue in new section 340A of the CSA, for the Committee's consideration.

Information Privacy Act 2009

Queensland's *Information Privacy Act 2009* (**IP Act**) recognises the importance of protecting the personal information of individuals. It creates a right for individuals to access and amend their own personal information and provides rules or 'privacy principles' that govern how Queensland government agencies collect, store, use and disclose personal information. OIC has regulatory oversight of Queensland Government agencies' compliance with requirements under the IP Act.

The Office of the Information Commissioner is an independent statutory authority.

The statutory functions of the OIC under the Information Privacy Act 2009 (Qld) (IP Act) include commenting on the administration of privacy in the Queensland public sector environment.

This submission does not represent the views or opinions of the Queensland Government.

Clauses 16 to 20 and 36 of the Bill – Use of x-ray body scanners and other emerging technologies

Imaging searches

Clauses 16 and 18 of the Bill amend sections 159 and 173 of the CSA to authorise the chief executive to require an imaging search to be conducted on visitors and staff members attending at corrective services facilities, respectively. Clause 36 of the Bill defines an 'imaging search' as *'…a search of the person using electronic*

imaging produced by a method of scanning the person, including, for example, using non-ionising radiation'.

The Bill introduces a new section 175A into the CSA regulating the conduct of searches. Controls imposed by this section include:

- an obligation to ensure as far as reasonably practicable, that a person subject to a search is searched in a way that causes minimal embarrassment to the person and to minimise any physical contact with the person[1]
- provision that only a device prescribed by regulation may be used to conduct an imaging search of a person;[2] and
- provision that regulation may prescribe additional limitations on the use of imaging searches, such as prescribing:
    - the maximum number of a times a person may be searched using a particular device in a stated period;[3] and
    - other procedures relating to imaging searches, including for the use, storage and destruction of any images produced by the scan.[4]

OIC would welcome the opportunity to be further consulted in the development of any regulations prescribing limitations on imaging searches, including any relevant exclusions that may apply;[5] and rules concerning use, and retention of images produced by a scan.

Surveillance devices

Clause 19 of the Bill introduces a new chapter 4, part 3A into the CSA, which will allow for the electronic surveillance of corrective services facilities using surveillance devices to be prescribed by regulation. OIC notes surveillance device is broadly defined in the Bill to mean a device capable of transmitting or recording sound, images, or changes in an environment.[6]

OIC understands that the above will authorise the use of surveillance and other technologies such as BWCs, camera drones and CCTV to capture and record video and audio in and around corrective services facilities. OIC understands that these amendments are intended to provide clear authority for the use of surveillance and emerging technologies and the information they record in corrective services facilities to maintain safety and monitor threats within the closed correctional environment.[7]

The use of surveillance devices and other emerging technologies such as BWCs and CCTV pose a number of privacy risks to an individual. Further, the information generated using these technologies will include personal information, enlivening the privacy obligations in the IP Act and rendering collected information subject to the rights of access and amendment conferred by the IP Act and *Right to Information Act 2009* (**RTI Act**).

As part of its statutory functions, OIC has produced guidelines for agencies outlining the privacy impacts and information access obligations agencies must consider when implementing or extending a camera surveillance system (including

---

[1] The new section 175A(1) of the CSA.
[2] The new section 175A(4) of the CSA.
[3] The new section 175A(5)(a) of the CSA.
[4] The new section 175A(5)(b) of the CSA.
[5] For example, persons fitted with a medical implant. On this point, OIC notes the advice in the Explanatory Notes that the proposed power to conduct imaging searches '*…is subject to any other regulation or laws governing use of such technology, including requirements under the* Radiation Safety Act 1999 *(RSA) and* Radiation Safety Regulation 2021*. Body scanning technology may only be used…if these other stringent regulatory requirements are met*' (page 8).
[6] New section 173A(6) of the CSA.
[7] Explanatory Notes, page 1.

BWCs).[8] We note that a number of OIC audits have found Queensland government agencies continue to need to improve maturity of systems, processes and practices for video surveillance to ensure compliance with the RTI and IP Acts and good practice.[9]

For this reason OIC recommends that any agency considering the use of surveillance devices conduct a Privacy Impact Assessment (**PIA**) before using these technologies. While the collection of personal information using these technologies may be considered necessary to better achieve the objects of the CSA, it should be appropriately balanced so as not to intrude unreasonably into the personal affairs of prisoners, visitors and staff. A PIA will assist to identify privacy risks and appropriate mitigation strategies. OIC considers appropriate safeguards include robust operational procedures, training and auditing to prevent unauthorised access to or misuse of personal information collected through the adoption of these technologies. The PIA should be updated at key phases throughout the lifecycle of the implementation and use of surveillance technologies, including the passing of the legislation and prior to adoption of any new surveillance technologies.

As with provisions concerning imaging scanning, OIC welcomes the various limits and safeguards on the use of surveillance devices proposed in the Bill, including:

- restrictions on the use of covert surveillance;[10] and
- ensuring[11] that the use of prescribed surveillance devices under new section 173A of the CSA is subject to existing restrictions and obligations about recording and monitoring prisoner communications, as prescribed in existing section 52 of the CSA.[12]

OIC further supports:

- the mandatory requirement for the chief executive to have regard to various matters prior to authorising the use of prescribed surveillance devices within a facility,[13]
- the express requirement for the chief executive to consider the privacy of prisoners, corrective services officers and visitors to the facility,[14] and
- the obligation to include in any authorisation requirements about the use, storage and destruction of the resulting recordings.[15]

OIC would welcome the opportunity to provide comment on requirements about the use and retention of recordings to be developed under the proposed section 173A(2) of the CSA.

---

[8] https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/camera-surveillance-and-privacy.

[9] *Camera surveillance and privacy,* Office of the Information Commissioner Queensland, Report No. 2 of 2012/13 to the Queensland Legislative Assembly; *Camera surveillance and privacy – follow-up review*, Office of the Information Commissioner Queensland, Report No.1 of 2015-16 to the Queensland Legislative Assembly; *10 years on: Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld),* Office of the Information Commissioner Queensland, Report No. 5 to the Queensland Legislative Assembly for 2018-19.

[10] The chief executive being precluded, under new section 173A(3)(b), from authorising the covert use of a surveillance device (as defined in new section 173A(4)), unless such use is otherwise authorised under another provision of the CSA or another enactment.

[11] Under new section 173A(5)(c) of the CSA.

[12] Section 52(2) of the CSA requires that authorised prisoner communications between a prisoner and their lawyer, an officer of a law enforcement agency, the parole board or the ombudsman must not be recorded or monitored. Section 52(3) requires that the parties to each prisoner communication must be told the communication may be recorded and monitored.

[13] The new section 173A(1)(a) to (d) of the CSA.

[14] The new section 173A(3)(c) of the CSA.

[15] The new section 173A(2) of the CSA.

As a final comment on this specific issue of surveillance, OIC draws the Committee's attention to additional safeguards applying in a similar context, as contained in the *Youth Justice Act 1992* (Qld) (**YJ Act)**. These are prescribed in section 263B of that Act, and oblige the chief executive to:

- make guidelines about the recording of images and sounds in detention centres and the use of BWCs by detention centre employees;[16] and
- ensure that a child detained in a detention centre, a detention centre employee and a visitor to a detention centre are advised that sounds and images may be recorded.[17]

Clauses 31 to 32 of the Bill - new information sharing framework

Clauses 31 and 32 establish an information sharing framework, generally permitting a more liberal sharing of prisoners' personal information than is currently permitted under the existing legislative framework.[18] As the proposed amendments currently stand, such information – some of which may include sensitive health information – could be disclosed without the consent of those to whom it relates, posing a risk to the information privacy of those individuals.[19]

OIC appreciates that a key aim of these amendments is to promote prisoner health and wellbeing, support frontline service delivery and interagency collaboration.[20]

OIC further notes the right to privacy is not absolute. An appropriate balance must be struck between privacy and other legitimate rights and interests. While the right to privacy can be limited, any interference must be reasonable, necessary, and proportionate to achieving a legitimate policy goal.

The Bill includes a number of safeguards that apply to the sharing of information: OIC notes and supports the various constraints prescribed in the new sections 341(3)(g) to 341(3)(i), for example, and the restrictions imposed by new section 340A.

OIC does consider, however, that the proposed information sharing provisions, particularly in relation to health information, could be strengthened by inclusion of in the Bill of a 'consent wherever possible' principle, requiring those contemplating the disclosure of prisoner personal information to obtain consent beforehand, where possible.

A model in this regard can be found in section 297C of the YJ Act. This provision contains a principle for information sharing which provides that whenever possible and practical, a person's consent should be obtained before disclosing confidential information. Section 297C(2) of the YJ Act further provides that section 297C does not prevent information relating to a person from being disclosed if the person's consent is not obtained before the disclosure.

OIC considers the above principle to be particularly important as regards disclosure of information to a health practitioner for the care and treatment of a

---

[16] Section 263B(1) of the YJ Act.
[17] Section 263B(2) of the YJ Act. On this point, OIC does note the statement in the Explanatory Notes that '[e]*ach corrective services facility already has clear signage notifying prisoners, staff and visitors that they are under audio and visual surveillance while on the premises. This signage provides that recorded material will only be accessed by persons authorised to do so and will be handled in accordance with the* Information Privacy Act 2009 *and CSA (section 341)*'.
[18] Specifically, increased information sharing with law enforcement agencies and information sharing in prison transfers or when a prisoner is to be removed from Australia to another country.
[19] A matter recognised in the Explanatory Notes, page 17, where it is stated that proposed '*disclosure of information may be considered inconsistent with rights and liberties of individuals…given the amendments enable the disclosure of private or confidential information without requiring the person's consent.*'
[20] Explanatory Notes, page 1.

prisoner.[21] There is likely to be a broad range of health information that could be shared about a prisoner, not limited to circumstances where it is not possible or practicable to obtain the prisoner's consent prior to disclosure. In these circumstances, OIC's submission is that the consent of the prisoner should be sought, wherever practicable, prior to the sharing of the prisoner's health information.

In making this comment, OIC notes the observations in the Statement of Compatibility[22] accompanying the Bill (**SoC**) that while:

> *…prisoner consent is preferred in the first instance, this may not always be possible. For example, a prisoner may not have capacity to provide consent (i.e. unconscious), or may be unwilling to disclose the information (such as where they are suspected of ingesting contraband). Requiring consent would not be as effective in achieving the intended outcome.*[23]

Adopting a consent principle analogous to section 297C of the YJ Act would not, however, preclude disclosure in circumstances such as those noted in the SoC. It prescribes a principle informing disclosure, rather than a prohibition on disclosure, which emphasises the desirability of obtaining consent where possible, while allowing disclosure in circumstances – such as those noted in the SoC - where obtaining consent is not possible.

Other issues

Definitional issue in new section 340A

The Bill introduces a new section 340A into the CS Act prohibiting the disclosure of 'sensitive information from law enforcement agencies'.[24]

The definition of 'sensitive law enforcement information' adopts the wording of schedule 3, section 10 of the RTI Act, including providing that such information means:

> *information obtained, used or prepared—*
>
> *(i) for an investigation by a part of the police service known as the State Intelligence Group; or*
> *(ii) for an investigation by a part of the police service known as the State Security Operations Group; …*

The 'State Security Operations Group' referred to in new section 340A(c)(ii) of the CSA does not exist; a matter canvassed by OIC in our 5 August 2022 submission responding to the Department of Justice and Attorney-General's Consultation Paper 'Proposed changes to Queensland Information Privacy and Right to Information Framework':[25]

> *Schedule 3, section 10(5)(b) of the RTI Act refers to the 'State Security Operations Group'. Queensland Police Service (QPS) has confirmed that the State Security Operations Group (**SSOG**) no longer exists and the functions of the SSOG moved to the Security Investigations Team. OIC recommends consulting with QPS and amending section 10(5)(b) of the RTI Act to remove reference to the SSOG and replace it with the appropriate title to avoid uncertainty around the application of section 10(5)(b) of the RTI Act.*

---

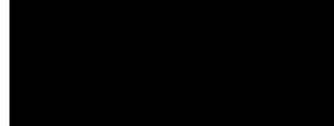
[21] As envisaged by the new section 341(3)(g) of the CSA.
[22] Prepared in accordance with Part 3 of the *Human Rights Act 2019* (Qld).
[23] Page 26.
[24] Clause 31.
[25] See page 34 of OIC's submission, accessible at https://www.oic.qld.gov.au/__data/assets/pdf_file/0016/53017/submission-public-consultation-paper-RTI-IP-Acts.pdf

The above observations would appear to apply equally to the proposed section 340A(c)(ii) of the CS Act.

Conclusion

OIC welcomes the opportunity to make the foregoing submission and remains available to provide any further assistance to the Committee in its consideration of the Bill.

Yours sincerely



Paxton Booth
Acting Information Commissioner

Susan Shanley
Acting Privacy Commissioner