Queensland Human Rights Commission

Our ref: BNE3416944

3 December 2019

Operation Impala
Crime and Corruption Commission
GPO Box 3123
Brisbane Qld 4001

By email only: operationimpala@ccc.qld.gov.au

Dear Sir/Madam

Submission to Operation Impala: An examination of corruption and corruption risks in relation to the improper access to and disclosure of confidential information in the public sector

Thank you for this opportunity to supplement my oral evidence presented at the investigative hearing of Operation Impala on 22 November 2019.

Introduction

1. The Queensland Human Rights Commission (**QHRC**) is a statutory authority established under the Queensland *Anti-Discrimination Act 1991*.

2. The functions of the QHRC include promoting an understanding, acceptance, and public discussion of human rights in Queensland. From 1 January 2020, the QHRC will deal with human rights complaints made against public entities, and have a role in reviewing public entity policies, programs, and procedures in relation to their compatibility with human rights.

3. Also from 1 January 2020, the *Human Rights Act 2019* (Qld) (**HRA**) will require:

    a. public entities to act compatibly with and make decisions that give proper consideration to human rights;
    b. proposed legislation to be scrutinised for compatibility with human rights; and
    c. courts and tribunals to interpret legislation in a way that is compatible with human rights.

4. 'Compatible with human rights' means that the act, decision, or legislative provision does not limit a human right, or if it does limit a human right, then only to the extent that is reasonable and demonstrably justifiable.

STATEWIDE
tollfree
1300 130 670
info@qhrc.qld.gov.au
qhrc.qld.gov.au
fax 07 3193 9979

Brisbane
Level 20
53 Albert Street
Brisbane Q 4000
PO Box 15565
City East Q 4002

Cairns
Ground Floor
10 Grove Street
PO Box 4699
Cairns Q 4870

Townsville
Ground Floor
187-209 Stanley Street
PO Box 1566
Townsville Q 4810

Rockhampton
Level 1
209 Bolsover Street
PO Box 1390
Rockhampton Q 4700

The right to privacy under the HRA

5. Section 25 of the HRA provides:

> **25 Privacy and reputation**
> A person has the right—
> (a) not to have the person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
> (b) not to have the person's reputation unlawfully attacked.

6. Based on international case law, the right to privacy may be interpreted as placing a positive responsibility on government to do what is necessary and reasonable to protect private information.

7. For example, in *S and Marper v United Kingdom* [2008] ECHR 1581, the applicants had fingerprints and DNA samples taken when they were arrested, but were never convicted. When the applicants requested that the fingerprints and samples be destroyed, the police refused. In considering the scope of Article 8 of the *European Convention of Human Rights*[1], the Court said:

> 103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse ...

8. The Court did not, however, need to comment on the adequacy of the safeguards in this case, finding instead that:

> 125. … the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants'; right to respect for private life and cannot be regarded as necessary in a democratic society.

9. In *MM v United Kingdom* [2012] ECHR 1906, the lack of legislative framework for the collection and storage of criminal record data, and the lack of clarity regarding powers to

[1] **Right to respect for private and family life**
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

retain and disclose that data, was in violation of the applicant's right to respect for private life. Coming to this conclusion, the Court said:

> 199. … the indiscriminate and open-ended collection of criminal record data is unlikely to comply with the requirements of Article 8 in the absence of clear and detailed statutory regulations clarifying the safeguards applicable and setting out the rules governing, *inter alia*, the circumstances in which data can be collected, the duration of their storage, the use to which they can be put and the circumstances in which they may be destroyed.
>
> 200. Further, the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data. The Court considers that the obligation on the authorities responsible for retaining and disclosing criminal record data to secure respect for private life is particularly important, given the nature of the data held and the potentially devastating consequences of their disclosure.

10. Following these authorities, the right to privacy under the HRA may require public entities to have adequate procedural safeguards against unauthorised access and disclosure of stored personal information. The level of protection necessary will depend upon the nature of the information collected, the purpose for which it is collected, and the harm that may be caused if privacy is breached. It will not be sufficient for public entities to only have policies in place; they must also take reasonable steps to ensure the policies are followed. Failure to provide adequate safeguards may amount to a disproportionate and therefore unlawful limitation of a person's right to privacy. Matters that may need to be considered include how information is stored, duration, usage, access by third parties, procedures to preserve the integrity and confidentiality of data, and procedures for destruction.[2]

11. Information Privacy Principle 4[3] and National Privacy Principle 4[4] contained in Schedules 3 and 4 to the *Information Privacy Act 2009* (Qld) (**IPA**) place a positive obligation on agencies to take reasonable steps to protect personal information and safeguard against misuse. The HRA will help inform the interpretation of what is 'reasonable', having regard to human rights and the factors described above.

Enforcement action when misuse occurs

---

[2] See *S and Marper v United Kingdom v United Kingdom* [2008] ECHR 1581 at [99].

[3] **IPP 4—Storage and security of personal information**

(1) An agency having control of a document containing personal information must ensure that—
  (a) the document is protected against—
    (i) loss; and
    (ii) unauthorised access, use, modification or disclosure; and
    (iii) any other misuse; and
  (b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.
(2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

[4] **NPP 4—Data security**

(1) A health agency must take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure.
(2) If the personal information is no longer needed for any purpose for which the information may be used or disclosed under NPP 2, the health agency must take reasonable steps to ensure that the individual the subject of the personal information can no longer, and can not in the future, be identified from the personal information. (note omitted)

12. Human rights need to be considered by public entities in their decision-making regarding the consequences of improper access, use, and disclosure of confidential information.

13. As pointed out in the Operation Impala call for public submissions dated 20 September 2019, improper access and misuse of personal information can have serious and far-reaching consequences for the individual to whom the information relates, impacting on rights beyond the right to privacy and reputation. For example, improper access of information by Queensland Corrective Service staff can result in safety and security concerns for individual prisoners, triggering the rights to recognition and equality before the law[5], protection from torture and cruel, inhuman or degrading treatment[6], liberty and security of person[7], and humane treatment when deprived of liberty.[8] A police officer who accesses confidential information relevant to legal matters they are personally involved in engages the right to a fair hearing.[9]

14. When unlawful access or use of personal data has been identified, public entities must respond having regard to the human rights that have been engaged. Failure to take disciplinary or criminal action, or failing to review processes to avoid future wrongdoing, may be a disproportionate limitation of human rights.

15. Many victims are likely to be already vulnerable and suffering multiple disadvantages, and will not have the personal or financial resources to commence their own legal proceedings for breach of privacy or confidence. Existing statutory and common law protections provide no deterrent value if they are not pursued.

Strengthening protections under the IPA

16. The IPA provides access for individuals with a privacy complaint to mediation with the Office of the Information Commissioner and, if unsuitable for or unsuccessful at medication, to a hearing for determination by QCAT. A privacy complaint is one in which a relevant entity is alleged to have not complied with the privacy principles in relation to the complainant's personal information.[10]

<u>Privacy principles</u>

17. NPP4 provides that once personal information has fulfilled its purpose, the health agency must take reasonable steps to ensure that it is de-identified. The IPP does not appear to have any comparable provision. In overseas jurisprudence, the longer the retention times, the stronger the safeguards need to be. The privacy principles could be reformed to make express reference to retention times, subject to the requirements of the *Public Records Act 2002* (Qld).

[5], HRA s 15.
[6], HRA s 17.
[7] HRA s 29.
[8] HRA s 30.
[9] HRA s 31.
[10] See IPA ss 164 – 178.

18. While the privacy principles provide limits on the 'use' of personal information only for a relevant purpose, it does not expressly refer to 'access' by people other than the person to whom the information relates. The privacy principles could strengthen expectations about access to information by unauthorised persons.

Individual and vicarious liability

19. The IPA does not allow for direct liability of individuals. Only 'relevant entities' can be liable for breach of the privacy principles, and individual employees are not relevant entities. Individual liability under the IPA would mean more accessible dispute resolution processes for complainants, and provide a further deterrent for misconduct that is not reliant on the public entity taking criminal or disciplinary action.

20. If liability for individuals under the IPA was implemented, then it would also be appropriate to include a provision that clarifies the vicarious liability of the principal. Under the *Anti-Discrimination Act 1991* (Qld), a principal will be liable for the actions of its workers or agents taken in the course of work or while acting as agent. It is a defence if the principal proves, on the balance of probabilities, that it took reasonable steps to prevent the lawyer or agent from contravening the Act.[11]

Remove cap on compensation

21. The current limit on compensation under the IPA is $100,000, which has been in place since the Act's commencement on 12 June 2009. This figure is inclusive of any legal costs, economic loss, and non-economic loss. There is no explanation for the limit in the Explanatory Memorandum.

22. The Australian Law Reform Commission, in their inquiry into a stand-alone tort for serious invasions of privacy[12], recommends only limiting non-economic loss at a level equivalent to the limit on non-economic loss in defamation, currently $407,500 under the *Defamation Act 2005* (Qld). The IPA could adopt a similar approach.

Objects of the IPA

23. The primary object of the IPA is to provide for:

> (a) the fair collection and handling in the public sector environment of personal information; and
> (b) a right of access to, and amendment of, personal information in the government's possession or under the government's control unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended.[13]

[11] *Anti-Discrimination Act 1991* (Qld) s 133.
[12] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, 3 September 2014).
[13] IPA s 3.

24. A human rights approach to applying the IPA would be assisted by expressly identifying the purpose and values that underpin this object, for example:

    a. Safeguards the rights of people in respect of their private information.
    b. Promotes community trust in the public sector.

Cultural change that respects and promotes human rights

25. A primary objective of the HRA is to help build a culture that respects and promotes human rights in the Queensland public sector.[14]

26. Human rights already underpin the privacy principles of the IPA, reflecting the Australian Privacy Principles of the *Privacy Act 1988* (Cth) which were drafted to give effect to Australia's obligations under the right to privacy stated in Article 17 of the *International Covenant on Civil and Political Rights*.

27. The implementation of the HRA is an opportunity to revisit the purpose and importance of privacy when dealing with confidential information and provide an ethical framework that supports fair decision-making, where individual rights are considered and balanced against organisational need and efficiency. A genuine commitment to this approach cannot be achieved through policy alone. Policies need to be supported by understanding and leadership from senior officers, and training for all staff.

28. Such measures to protect personal data are increasingly important as the use of mass surveillance and facial recognition, automation, profiling, artificial intelligence, and the use and storage of metadata continues to grow.

Yours sincerely

Scott McDougall
Commissioner

[14] HRA s 3(b).