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

15 February 2019

The Secretary
Queensland Law Reform Commission
PO Box 13312
George Street Post Shop
BRISBANE QLD 4003

By email: lawreform.commission@justice.qld.gov.au

Dear Secretary

Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies

The Office of the Information Commissioner (**OIC**) welcomes the opportunity to make a submission in response to the Queensland Law Reform Commission's (**QLRC**) Consultation Paper outlining important issues raised in the review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies.

OIC's submission

OIC's submission contains the OIC's general observations regarding Queensland's law relating to civil surveillance and the protection of privacy in the context of current and emerging technologies and OIC's comments in response to questions posed in the Consultation Paper.

OIC's general comments and responses to consultation questions in the Consultation Paper are **attached**.

If you would like to discuss any of the issues raised in OIC's feedback, please contact Susan Shanley, Principal Policy Officer via email Susan.Shanley@oic.qld.gov.au or by phone on (07) 3234 7373.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

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

The statutory functions of the OIC under the *Right to Information Act 2009* (Qld) and *Information Privacy Act 2009* (Qld) include commenting on the administration of right to information and privacy in the Queensland public sector environment.

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

Summary

I. The Office of the Information Commissioner Queensland (**OIC**) welcomes the release by the Queensland Law Reform Commission of the Consultation Paper on the *Review of Queensland's laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies* (**Consultation Paper**).

II. As noted in the Consultation Paper, privacy is recognised in international human rights instruments to which Australia is a signatory, including the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights 1966* (**ICCPR**). Article 17 of the ICCPR provides that:

1. *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, not to unlawful attacks on his honour and reputation*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

III. Article 17 of the ICCPR 'demonstrates that privacy is an important human right warranting recognition and protection'.[1] While the right to privacy under international human rights law is not absolute, 'any instance of interference must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality'.[2]

IV. 'Protection from surveillance is a fundamental form of protection of privacy, particularly in the digital era. Surveillance laws protect other freedoms as well. Unauthorised surveillance may interfere with freedom of speech, freedom of movement and association'.[3]

V. In her opening remarks, the United Nations High Commissioner for Human Rights (Commissioner) to the *Expert Seminar on the Right to Privacy in the Digital Age*, stated that 'ensuring the protection of individuals against any unlawful or arbitrary interference resulting from surveillance measures demands the presence of national legal frameworks. In addition, a lack of effective oversight and review to monitor compliance and enforcement contributes to a lack of accountability for arbitrary to unlawful intrusions on the right to privacy'.[4]

VI. Existing and emerging technologies with advanced image and audio capabilities pose a serious threat to an individual's privacy. Significant gaps exist in the current legislative framework regarding intrusions into the privacy of an individual. While there is a range of Commonwealth, State and Territory statutes and common law principles, the laws are complex, at times outdated by emerging technology, and significant variations exist between jurisdictions.[5]

VII. As noted in the Australian Competition and Consumer Commission's (**ACCC**) preliminary report on its *Digital Platforms Inquiry*, it has been the consistent finding of a number of legislative reviews that Australia's privacy regulatory framework does not provide consumers with adequate remedies for invasions of privacy. In its report, the ACCC cites the following examples:[6]

---

[1] Submission by the Office of the Australian Information Commissioner to the Attorney-General's Department, A Commonwealth statutory cause of action for serious invasion of privacy at page 10.
[2] United Nations Human Rights, Office of the High Commissioner, *The Right to Privacy in the Digital Age*, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
[3] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [13.6]-[13.7].
[4] Opening Remarks by Ms Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Palais des Nations, Geneva accessed at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E
[5] Drones and Privacy, Chapter 4, Eyes in the Sky Report.
[6] Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Preliminary Report at p.222.

- The NSW Legislative Council's inquiry on *Remedies for the serious invasion of privacy in New South Wales* found that 'there remain significant gaps in the coverage afforded to privacy protection'.[7] The inquiry found that the existing privacy framework in NSW (which includes the federal Privacy Act) does not provide adequate remedies to many people who suffer a serious invasion of privacy'.[8]

- The Australian Law Reform Commission's (**ALRC**) report on *Serious Invasions of Privacy in the Digital Era* found that 'although the existing law provides protection against some invasions of privacy, there are significant gaps or uncertainties'.[9] In particular, the ALRC found that the *Privacy Act 1988* (Cth) only provides for 'limited civil redress' by way of complaints made to the Australian Information Commissioner. The Privacy Act 'does not generally apply to the intrusions into personal privacy or to the behaviour of individuals or media entities, and does not generally apply to businesses with an annual turnover of less than $3 million'.[10]

VIII. The Queensland Drones Strategy, released in June 2018, notes concerns regarding the adequacy of Queensland's legislation to protect the privacy of individuals with the emergence of new technology.[11]

IX. The former Australian Information and Privacy Commissioner noted that the 2017 Australian Community Attitudes to Privacy Survey[12] shows that 'Australians are increasingly concerned about the privacy risks that have evolved in tandem with new technology and new ways of connecting socially'.[13]

X. Queensland's *Information Privacy Act 2009* (**IP Act**) plays a key role in safeguarding the rights of community members' personal information and provides clear principles and rules to guide appropriate behaviour by public sector agencies.

XI. However, the privacy protections in the IP Act are limited to Queensland government agencies and the regulation of information privacy. It does not regulate other types of privacy such as territorial and physical or bodily privacy. Other Queensland laws relevant to surveillance and privacy which might apply include:

- Section 227A of the *Criminal Code 1889*
- Chapter 33A of the *Criminal Code 1889*
- *Invasion of Privacy Act 1971*
- Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Act 2018;[14] and

[7] Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales Report*, (3 March 2016) at page 57.
[8] Standing Committee on Law and Justice, Parliament of New South Wales, Remedies for the serious invasion of privacy in New South Wales Report, (3 March 2016) at page 57.
[9] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [3.50].
[10] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [3.50].
[11] https://www.premiers.qld.gov.au/publications/categories/plans/queensland-drones-strategy.aspx.
[12] *Australian Community Attitudes to Privacy Survey 2017*, Office of the Australian Information Commissioner, https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017.
[13] Commissioner's foreword, *Australian Community Attitudes to Privacy Survey 2017*, Office of the Australian Information Commissioner, https://www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017
[14] Passed by the Queensland Parliament on 13 February 2019.

- Human Rights Bill 2018, which proposes a 'right to privacy and reputation' and requires public entities to act in a way that is compatible with human rights.

XII. OIC provides in-principle agreement with the preliminary view formed by the QLRC[15] that:

- considering the gaps, inconsistencies and uncertainties in the current legal framework in Queensland, a new legislative framework to protect the privacy of individuals in the context of the use of civil and surveillance devices and technology is necessary.
- the legislation should be sufficiently broad in its scope to regulate existing and emerging surveillance technologies and strike a balance between the interests in the use of surveillance and the privacy rights and interests of individuals who may be harmed or affected if surveillance is unreasonably intrusive. It should also aim to achieve reasonably consistency with the regulation of civil surveillance in other Australian jurisdictions.

XIII. OIC notes that a number of the consultation questions seek input on the proposed legislative framework to balance the right to privacy for individuals with countervailing public interest considerations, including legitimate use of surveillance technology.

XIV. Both the *Right to Information Act 2009* (**RTI Act**) and IP Act balance the right to access government-held information and the protection of an individual's privacy with other legitimate rights and interests. As such, the RTI and IP Acts may provide a useful framework when seeking to balance the right to privacy with competing rights in any proposed legislative framework to regulate civil surveillance.

About the OIC

XV. The OIC is an independent statutory body that reports to Parliament. We have a statutory role under the RTI Act and the IP Act to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard personal information that they hold.

XVI. OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance, and compliance with, the RTI Act and the IP Act. Our office reviews agency decisions about access to information, mediates privacy complaints and monitors and reports on agency compliance to Parliament.

Overview of the *Information Privacy Act 2009*

XVII. Queensland's IP Act only applies to Queensland Government agencies, which include Ministers, Queensland State Government Departments, Local Government and Public Authorities.[16] The IP Act does not apply to Government Owned Corporations (GOCs), individuals, the private sector or community organisations unless a contracted service provider is contractually bound to comply with the privacy principles.

XVIII. Queensland GOCs, the private and community sector could be covered under the Commonwealth's privacy legislation if these entities have an annual turnover of more than $3 million per annum.

[15] Consultation Paper at page 48.

[16] The IP Act also applies to contractually bound service providers.

XIX. The IP Act provides a right for individuals to have their personal information collected and handled in accordance with certain rules or 'privacy principles'. The IP also creates a right for individuals to make a privacy complaint to an agency if they consider that a Queensland Government agency has failed to comply with its obligations under the Act. If the complainant is not satisfied with the response, they can make a complaint to OIC.

XX. If a settlement cannot be reached for an accepted complaint, the complainant can ask the Information Commissioner to refer the complaint to the Queensland Civil and Administrative Tribunal (**QCAT**). QCAT may find the complaint or any part of it proven. In that instance QCAT may make an order restraining the agency from repeating any act or practice, order the agency to carry out certain acts, award compensation to the complainant not exceeding $100,000 and/or make further orders against the agency.

CONSULTATION QUESTIONS

Scope of a new legislative framework

Q – 1 What considerations should apply to surveillance that is conducted in a public place?

1. 'The concept of 'privacy' is not easily defined, nor is it always clear when or whether a particular act will impinge upon one's privacy'.[17] 'Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used'.[18]

2. Privacy is fundamental human right recognised in a number of international instruments and treaties including Article 17 of the International Covenant on Civil and Political Rights. Privacy underpins human dignity and other key values such as freedom of thought, speech and self-expression and freedom of movement and association.

3. Attempts to define or conceptualise privacy have sometimes drawn on the distinction between what is 'public' and what is 'private'.[19] Gleeson CJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [20]stated:

> 'There is no bright line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private'.[21]

4. As noted in the Consultation Paper, distinguishing between what is 'private' and what is 'public' can be misleading since privacy can still have a role to play in public places.

> 'Protection of privacy is…not dependent on classification of physical spaces as public or private. It provides a choice over how, as individuals we interact with others, even in publically accessible locations'.[22]

5. As noted by the Victorian Law Reform Commission (**VLRC**), 'most, if not all, people would have reasonable expectations of some privacy in public places. The nature of those reasonable expectations will change according to time and place. Most people would reasonably expect, for example, that a conversation on a secluded park bench or quiet beach would not be overheard or recorded, and most people would similarly expect that a brief intimate moment, such as a kiss or embrace, in a secluded public place would not be observed or recorded. It

[17] Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales*, (3 March 2016) at page 17.
[18] IAPP, *What does privacy mean*? viewed at https://iapp.org/about/what-is-privacy/.
[19] Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales*, (3 March 2016), at page 17.
[20] (2001) 208 CLR 199, [42] cited in Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales*, (3 March 2016) at page 17.
[21] (2001) 208 CLR 199, [42] cited in Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales*, (3 March 2016)at page 17.
[22] Consultation Paper at [2.6].

may be unreasonable to have similar expectations on a crowded tram or in a busy shopping mall'.[23]

6. Cultural differences in privacy exist and the distinction between what is 'private' and what is 'public' will vary according to social and cultural norms. The Australian Law Reform Commission (**ALRC**) in its report on *Serious Invasions of Privacy in the Digital Era*[24] noted that some information may be considered to be more private in some cultures than others. For example, 'the cultural expectations of Aboriginal and Torres Strait Islander peoples and other cultural or ethnic groups may be relevant to the reasonable expectation of privacy in some circumstances'.[25]

7. The VLRC further noted that 'the need to retain privacy in public places is sometimes concerned with the desire to keep particular information private'.[26] This information may relate to a person's political views, medical issues or other social matters. The VLRC concluded 'that is strongly arguable that people ought to be able to restrict access to information about themselves of this nature'.[27]

8. 'Recent advances have made surveillance technology—ranging from familiar tools such as CCTV to more sophisticated technologies such as drones and facial recognition, a form of biometric technology—more readily available, affordable and sophisticated'.[28] Combining these technologies allows for the creation of devices with increased surveillance capabilities. 'A consequence of the convergence of surveillance technologies is the greater ability of surveillance users to compile detailed pictures of members of the public, making It increasingly difficult for individuals to maintain their privacy and anonymity'.[29]

9. For example, the proposal by Moreton Bay Council to install CCTV in public places with audio and video capability generated significant public debate regarding the right to privacy in public places. Increasingly sophisticated surveillance technology has the ability to intrude on a person's privacy in public spaces, blurring the lines between 'private' and 'public'.

   OIC concurs with QLRC's view that legislation should regulate surveillance by reference to reasonable expectations of privacy; surveillance is part of everyday life and not all surveillance should be restricted.[30] Cultural considerations are also likely to be relevant, including the type of information or activity considered 'private' or 'sensitive'. China's social credit system highlights differing societal expectations about acceptable levels of surveillance. Also, the issue of consent, including parental consent, to surveillance poses additional challenges.

10. OIC notes the VLRC proposed a principle-based, outcome-focused approach to regulation of public place surveillance and devised a set of overarching principles for inclusion in legislation

[23] Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (June 2010) at [4.31].
[24] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014).
[25] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [6.70].
[26] Victorian Law Reform Commission, *Surveillance in Public Places*: Report No 18 (June 2010) at [4.34].
[27] Victorian Law Reform Commission, *Surveillance in Public Places*: Report No 18 (June 2010) at [4.34].
[28] Victorian Auditor-General's Report, *Security and Privacy of Surveillance Technologies in Public Places*, September 2018, [1.1].
[29] Victorian Law Reform Commission, *Surveillance in Public Places*: Report No 18 (June 2010) at [2.6].
[30] Consultation Paper at [3.15].

that seek to balance competing rights and interests.[31] The six public place surveillance principles devised by the VLRC are:

I. People are entitled to a reasonable expectation of privacy in public places.
II. Users of surveillance devices in public places should act responsibly and consider the reasonable expectations of privacy of individuals.
III. Users of surveillance devices in public places should take reasonable steps to inform people of the use of those devices.
IV. Public place surveillance should be for a legitimate purpose related to the activities of the organisation conducting it.
V. Public place surveillance should be proportional to its legitimate purpose.
VI. Reasonable steps should be taken to protect information gathered through public place surveillance from misuse or inappropriate disclosure.

11. OIC further notes that the ALRC in its inquiry into *Serious Invasions of Privacy in the Digital Era* recommended a non-exhaustive list of factors that a court may consider when determining whether a person would have had a reasonable expectation of privacy.

12. Accordingly, it is OIC's view that the following considerations should apply to surveillance in public places:

- whether an individual has a reasonable expectation of privacy (having regard to the range of factors outlined by the VLRC)[32]
- whether reasonable steps have been taken to inform the intended target of the use of those devices
- whether any interference with the right to privacy of an individual is necessary, undertaken for a legitimate purpose and proportionate to the legitimate purpose for which it is being used; and
- whether reasonable steps have been taken to protect information gathered through surveillance from misuse or inappropriate disclosure.

13. Proportionality is important to ensuring that a balance is achieved between safeguarding the privacy of individuals and other public interests, such as, the identification and prevention of crime and ensuring the safety of minors.

14. For example, it was recently reported that some Victorian private schools trialled facial recognition technology to scan classrooms for students' faces to monitor attendance in real time, in the absence of consent of either the parent or the child, as a replacement for calling the roll.[33] The use of facial recognition technology is privacy invasive and the public interest of ensuring student safety is outweighed by the compromising of children's privacy, including

[31] Victorian Law Reform Commission, *Surveillance in Public Places*: Report No 18 (2010) at [5.10].
[32] The Commission's view is that the reasonableness of any expectation of privacy in public will depend on, among other things, the following factors: the location; the nature of the activity being observed; whether the activity is recorded and disseminated; the type of surveillance used; the identity of the person being observed (for example a public official, celebrity or member of the public); whether the surveillance was harassing in nature; whether the surveillance was covert; whether the person specifically consented to the surveillance', Victorian Law Reform Commission, *Surveillance in Public Places*: Final Report 18 at [5.15].
[33] https://www.brisbanetimes.com.au/national/victoria/tough-new-rules-for-big-brother-face-reading-technology-in-schools-20190205-p50vpx.html.

the safety and security of biometric information. In this instance, the use of facial recognition technology was disproportionate to the purpose i.e. saving teachers up to 2.5 hours a week by replacing the need for them to mark the roll at the start of every class.

15. The roll-out of China's social credit scheme, enabled by rapid advances in facial recognition, body scanning and geo-tracking, to monitor and shape the behaviour of its citizens illustrates the impact on an individual's privacy when it is set aside for broader public interests. It also raises issues of consent and the use of surveillance in public places.

16. As noted in the Consultation Paper, legislation usually treats surveillance and the collection of personal information about an individual as an infringement of the person's privacy unless the person consents to it.[34] OIC agrees that as a general principle, surveillance should ordinarily be permitted if it occurs with consent. However, the concept of 'consent' is complex. Consent has been criticised, as it is not always specific, informed and freely given due to a range of factors, including imbalance in bargaining power.

17. For example, the Australian Competition and Consumer Commission (**ACCC**), in its preliminary report,[35] found considerable imbalance in bargaining power between digital platforms and consumers and criticised the use of click-wrap agreements with take-it-or-leave-it terms and bundled consents, which limits the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data.[36] Without adequate information, the ACCC concluded that consumers are unable to make informed decisions impeding potential competition between digital platforms on the privacy and data protection offered. The ACCC recommended (Recommendation 8(c)) amending the definition of consent to require express, opt-in consent and incorporate requirements into the Australian Privacy Principles that consent must be adequately informed, voluntarily given, current and specific.

18. Further, OIC considers that the use of surveillance devices in public places (and more broadly) should be transparent, accountable and subject to effective controls, oversight, complaint-handling investigation, sanctions and enforcement.[37] This should apply equally to covert surveillance conducted by law enforcement officers. The Public Interest Monitor's oversight functions concerning surveillance warrants by Queensland Police Service and the Crime and Corruption Commission provides a practical example.

Q – 2 What considerations should apply to surveillance that is conducted overtly or covertly?

19. Identified privacy risks arise through the use of overt and covert surveillance and their use should be regulated through legislation. Different considerations arise for surveillance that is conducted covertly given it 'represents a more significant invasion of individual privacy than

[34] Consultation Paper at [3.27].
[35] Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Preliminary Report, December 2018.
[36] Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Preliminary Report, December 2018 at page 8.
[37] Australian Privacy Foundation, Democratic Control of Surveillance by the State, https://privacy.org.au/policies/state-surveillance/

surveillance conducted overtly'.[38] Covert surveillance is usually conducted for law enforcement purposes with judicial oversight of the decision to conduct intrusive covert surveillance.

20. Accordingly, OIC concurs with the NSWLRC[39] that different levels of oversight and regulation are required based on whether the surveillance is overt or covert. The legislative principles set out by the NSWLRC to govern overt surveillance provide a useful framework for determining what considerations should apply to surveillance conducted overtly. They are:[40]

    1) Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.
    2) Overt surveillance must only be undertaken for a legitimate purpose.
    3) Overt surveillance must be conducted in a manner which is appropriate for purpose.
    4) Notice provisions shall identify the surveillance user.
    5) Surveillance users are accountable for their surveillance device and the consequences of their use.
    6) Surveillance users must ensure all aspects of their surveillance system are secure.
    7) Material obtained through surveillance to be used in a fair manner and only for the purpose obtained
    8) Material obtained through surveillance be destroyed within a specified period.

21. OIC accepts that covert surveillance may be justified in limited circumstances, such as law enforcement. Given the intrusive nature of covert surveillance, the conduct of covert surveillance requires a regulatory framework for the authorisation and oversight of this type of surveillance. This may include judicial oversight through the issuing of warrants and independent reporting on compliance with the proposed legislative framework regulating covert surveillance.

22. OIC notes that the NSWLRC considered that the 'type of authorisation required, and the body from which it should be obtained, would depend on whether the surveillance was being conducted by a law enforcement officer, in an employment context or in the public interest'.[41] Provision for emergency situations, where prior authorisation is not possible or practicable, was also contemplated.

23. In Queensland, the Public Interest Monitor[42]has a number of oversight functions with respect to surveillance warrants, for example, listening devices, tracking devices, optical surveillance devices or a combination of these devices obtained by the Queensland Police Service and the Crime and Corruption Commission. These functions include:

    - monitoring compliance by law enforcement officers with the chapter 13 of the *Police Powers and Responsibilities Act 2000* in relation to matters concerning applications for surveillance device warrants

[38] New South Wales Law Reform Commission, *Surveillance*, Report No 108 (May 2005) at page 4.
[39] New South Wales Law Reform Commission, *Surveillance*, Report No 108 (May 2005).
[40] New South Wales Law Reform Commission, *Surveillance*, Report No 108 at page 5.
[41] New South Wales Law Reform Commission, *Surveillance*: Report No 108 at page 5.
[42] The Public Interest Monitor is appointed under the *Police Powers and Responsibilities Act 2000* and the *Crime and Misconduct Act 2001*.

- approvals of the use of surveillance devices under emergency authorisations
- gathering statistical information about the use and effectiveness of covert search warrants and surveillance device warrants; and
- reporting requirements.

24. Other considerations that should apply to surveillance conducted covertly is whether an individual has a reasonable expectation of privacy. As outlined in the Consultation Paper, the greater expectation of privacy in a given situation, the less acceptable covert surveillance will ordinarily be.[43]

Q – 3 Should new legislation adopt the existing 'categories' approach used in other jurisdictions and define 'surveillance device' to mean:

a) a listening device;
b) an optical surveillance device;
c) a tracking device;
d) a data surveillance device;
e) other device (and if so, what should this be)?

25. OIC notes the existing categories approach used in other jurisdictions - as outlined in the Consultation Paper - to define a 'surveillance device'.

26. Consistency with privacy laws of other jurisdictions is important. This aligns with the view expressed by the ALRC in its review of *Serious Invasions of Privacy in the Digital Era* that 'consistency and uniformity in surveillance device laws and workplace surveillance laws is desirable'.[44] The ALRC noted that 'laws that are unnecessarily complex, fragmented and inconsistent impose an unnecessary regulatory burden on business. They also harm privacy…cause uncertainty and confusion, and make the law less effective'.[45]

27. While OIC accepts that privacy laws should be sufficiently flexible to adapt to rapidly changing technologies and capabilities, 'laws should be drafted with sufficient precision and definition to promote certainty as to their application and interpretation'.[46] In the absence of a clear statutory definition, the scope of the Bill will be uncertain and potentially open to challenge.

28. Further, failure to sufficiently define the meaning of 'surveillance device' in the legislation could lead to a range of unintended consequences given the broad range of devices with surveillance capabilities that can be used for legitimate purposes and are outside the intended scope of the regulatory framework.

[43] Consultation Paper at [3.25].
[44] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at 197.
[45] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [2.37].
[46] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [2.30].

29. For these reasons, OIC considers the legislation should adopt the existing 'categories' approach used in other jurisdictions to define 'surveillance device'. Surveillance technologies continue to evolve and any legislative definition must ensure that it encompasses future advances in these technologies. In OIC's view, enabling other devices to be prescribed by regulation provides the legislative framework with sufficient flexibility to keep pace with emerging surveillance technologies. OIC notes the risk, as outlined in the Consultation Paper, that the effectiveness of this approach requires ongoing monitoring by the legislature and the findings of several law reform commissions and other bodies that it is desirable for surveillance devices to be 'technology neutral' or 'non-device' specific, in order to keep pace with current and emerging technologies.[47]

Q – 4 If 'yes' to Q3:

a) how should each category of device be defined?
b) should each category of device be defined to extend to any particular technologies such as a program or system?
c) Should 'surveillance device' also include:
i. a combination of any two or more of those devices or technologies; or
ii. any other device or technology prescribed by regulation

30. 4a) and 4b) – see response to Q – 3.

31. OIC notes the legislation in New South Wales, the Northern Territory, South Australia and Victoria also defines a surveillance device to mean a combination of any two or more of those devices, and enables other kinds of devices to be prescribed by regulation.[48] OIC supports consistency and uniformity with privacy laws in other jurisdictions, where possible and practicable. According, OIC considers 'surveillance device' also include a combination of any two or more of those devices and any other device or technology prescribed by regulation.

Q – 5 Alternatively to Q -3, should new surveillance legislation adopt a 'technology neutral' approach and define 'surveillance device' to mean, for example, 'any instrument, apparatus, equipment or technology used either alone, or in combination, which is being used to deliberately monitor, observe, overhear, listen to or record an activity; or to determine or monitor the geographical location of a person or an object', or some other definition?

32. See response to Q-3.

[47] Consultation Paper at [3.33].
[48] Consultation Paper at [2.73].

The use of surveillance devices

Q-9 Should there be a general exception to the prohibition in Q-6 to permit participant monitoring

33. The *Invasion of Privacy Act 1971* does not prohibit the use of a listening device where the person using the listening device is a party to the private conversation.[49] OIC notes that other jurisdictions prohibit participant monitoring under their surveillance devices legislation. Only the Northern Territory and Victoria have similar participant monitoring exceptions to those in the Queensland legislation.

34. The VLRC in its review of *Surveillance in Public Places* formed the view that, 'as a rule, a person should be able to conduct private conversations and engage in private activities without those events being recorded without their consent. Such an expectation is consistent with the overall purpose of surveillance devices legislation, which is to protect privacy by prohibiting the covert use of surveillance devices other than in exceptional circumstances associated with law enforcement and recommended the general participant monitoring exception in the Victorian legislation be removed'.[50]

35. OIC concurs with the preliminary view of the QLRC that the proposed legislative framework in Queensland should not include a general exception for participant monitoring. OIC notes this approach is consistent with the surveillance devices legislation in several other jurisdictions, Commonwealth law regulating telecommunications and the position taken in other law reform reviews and inquiries that have considered this issue.[51]

36. Prohibiting 'participant monitoring' would bring Queensland in line with other jurisdictions and modernise Queensland's surveillance legislation to respond to increased capability of individuals to engage in surveillance due to advances in technology.

Q – 10 If 'no' to Q – 9, should there be any exceptions that permit participant monitoring in particular circumstances?

Q -11 If 'yes' to Q-10 what should be the particular circumstances for any exceptions and why? For example:

a) to protect a person's lawful interests;
b) where it is in the public interest;
c) where it is consistent with a person's safety or well-being (for example, where there is an imminent threat of violence or property damage, or to protect a child or adult with impaired capacity); or

[49] Section 43(2)(a).
[50] Victorian Law Reform Commission, *Surveillance in Public Places*: Final Report No 18 (2010) at [6.75].
[51] ALRC, NSWLRC and VLRC cited in the Consultation Paper at [3.99].

37. As outlined in the Consultation Paper, the majority of jurisdictions prohibit participant monitoring, and instead include exceptions that set out the circumstances in which a surveillance device may be used by a party.[52]

38. OIC accepts that, in some circumstances, it might be appropriate for a person to record a conversation to which they are a party without the knowledge or consent of other participants. OIC agrees with QLRC's view that 'these circumstances are more appropriately addressed by including specific exceptions in legislation'.[53] For example, as noted by the ALRC, 'media and journalistic activities offer significant public benefit, and these activities may at times justify the use of surveillance devices without the notice or consent of the individuals placed under surveillance. The removal of participant monitoring exceptions……would restrict the ability of journalists to use surveillance devices in this way'.[54]

39. Identifying the *particular* circumstances for any exceptions to a general prohibition on participant monitoring is complex and subject to divergent views by various bodies, including law reform commissions, that have conducted inquires and reviews on this issue.[55] Balancing the privacy rights of individuals with other legitimate rights and interests, such as public interest considerations, presents a number of challenges.

40. As noted by the NSWLRC, 'participant monitoring' is controversial because the interests that need to be protected or promoted are not easily distinguishable. Where a private conversation is recorded covertly by a third party, there is a clear breach of privacy and confidentiality. The only question is whether, and in what circumstances, that breach can be justified by other interests, such as the public interest in fighting crime. Where a private conversation is recorded by a party to that conversation without the knowledge or consent of the other parties, the situation is less clear'.[56]

41. Relevant exceptions to the general prohibition on 'participant monitoring' might include circumstances where it is reasonably necessary to protect a person's lawful interest; where it is in the public interest, and where it is consistent with a person's safety or well-being. While OIC considers specific exceptions should be legislated, OIC does not support the inclusion of overly broad exceptions, noting the concerns expressed by the ALRC and VLRC (as outlined in the Consultation Paper) about the potential consequences of an overly broad interpretation.

42. For example, The VLRC explained that it did not favour a broad interpretation of participant monitoring where it is to protect a person's lawful interests in order to keep an accurate

---

[52] *Listening Devices Act 1992* (ACT) s 4(1)(b), (2)–(4); *Surveillance Devices Act 2007* (NSW) s 7(1)(b), (2)–(3); *Surveillance Devices Act 2016* (SA) ss 4(1)(b), (2)–(3), 5; *Listening Devices Act 1991* (Tas) s 5(1)(b), (2)–(7); *Surveillance Devices Act 1998* (WA) ss 5(1)(b), (2)–(3), 6(1)(b), (2)–(3). In New South Wales, optical surveillance devices are treated differently: see Consultation Paper at Page 30.

[53] Consultation Paper at [3.104].

[54] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014) at [14.58].

[55] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Report No 123 (June 2014); Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (June 2010); D Stewart, 'Review of ACT Civil Surveillance Regulation' (Report, June 2016); New South Wales Law Reform Commission, *Surveillance: an interim report*, Report No 98 (February 2001); New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy Stage 3*, Report No 113 (January 2010).

[56] New South Wales Law Reform Commission, *Surveillance: an interim report*. Report No 98 (February 2001) at [2.100].

record[57] or an interpretation so narrow that it would exclude monitoring for evidentiary purposes.[58]

43. As stated by the New South Wales Court of Criminal Appeal *Sepulveda v the Queen*,[59] the lawful interests exception 'should not be interpreted in such a way as to render otiose the primary purpose of the Act, which is to protect privacy by prohibiting covert recording of a conversation other than (usually) by way of warrant under that Act'.[60]

44. The complexities of identifying particular circumstances for any exception to the general prohibition demonstrates that whether the surveillance activity is justified will depend on the context and circumstances of each particular case. Each case will require the balancing of competing rights and interests to determine if the incursion into an individual's privacy was necessary and proportionate to the protection of the relevant interest.

45. Privacy risks can be associated with permitting a person to engage in covert participant monitoring where it is not intended to communicate or publish to a person who is not a party. As noted by the VLRC, a person may have engaged in covert participant monitoring without the purpose of sharing the material with others however it is still possible that recordings made by a party to a conversation or activity 'may fall into the hands of third parties'.[61] This risk is exacerbated by the increasing availability of surveillance devices allowing information to be disseminated rapidly and with relative ease. When combined with the other known risks, such as the potential for unintentional or unauthorised access to this information, it is likely to result in undue interference with privacy.

Q – 15 Should there be a general prohibition on the communication or publication of information obtained through the unlawful use of a surveillance device? Why or why not?

46. Yes. As noted in the Consultation Paper[62]surveillance devices legislation generally prohibits the communication or publication of information obtained from the use of a surveillance device, except in certain circumstances.[63]

[57] This was proposed by the New Zealand Law Commission [3.93]-[3.94] cited in Consultation Paper at [3.118].
[58] Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (June 2010) [6.78]-[6.79] cited in Consultation Paper at [3.118].
[59] [2006] NSWCCA 379.
[60] *Sepulveda v the Queen* [2006] 167 A Crim R 108, [115], [142] 379, [142] cited in Consultation Paper at [3.114].
[61] Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (June 2010) at [6.81].
[62] Consultation Paper at [3.155].
[63] *Listening Devices Act 1992* (ACT) ss 5, 6; *Surveillance Devices Act 2007* (NSW) ss 11, 14; *Surveillance Devices Act* (NT) s 15; *Invasion of Privacy Act 1971* (Qld) ss 44, 45; *Surveillance Devices Act 2016* (SA) ss 9, 10, 12; *Listening Devices Act 1991* (Tas) ss 9, 10; *Surveillance Devices Act 1999* (Vic) s 11; *Surveillance Devices Act 1998* (WA) s 9 cited in Consultation Paper at [3.155].

47. Communication or publication of information obtained through the lawful and unlawful use of a surveillance device is privacy invasive. As outlined in the Consultation Paper, the purpose of legislative provisions is to prevent the limit or damage that could be caused by the communication or publication of information, obtained in this way, without consent.[64]

Q – 17 Should there be a general provision permitting the communication or publication of information obtained through the lawful use of a surveillance device? Why or why not?

48. No. As outlined in the response to Q -15, the surveillance legislation in other jurisdictions generally prohibits the communication or publication of information obtained through the use of a surveillance device, except in certain circumstances.

49. The provisions apply to information obtained from either the unlawful use or, except in New South Wales, the lawful use of a surveillance device. The purpose of these legislative provisions remains the same irrespective of whether the information was obtained through the lawful or unlawful use of a surveillance device.

Q – 18 If 'no' to Q-17, should the communication or publication of information obtained through the lawful use of a surveillance device be permitted in particular circumstances, for example if the communication or publication is made:

- **a) to a party or with the consent of the parties to the private conversation or activity;**
- **b) in the course of legal proceedings;**
- **c) to protect the lawful interests of the person making it;**
- **d) in the public interest;**
- **e) in connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;**
- **f) in the performance of a duty;**
- **g) to a person with a reasonable interest in the circumstances;**
- **h) by a person who obtained knowledge other than by the use of the device; or**
- **i) in any other circumstances?**

50. In certain circumstances, the communication or publication of information obtained through the use of surveillance device will justify an incursion on an individual's privacy. This position is consistent with provisions in other jurisdictions that 'set out a number of exceptions that permit a communication or publication, without consent, in particular circumstances in which the intrusion on privacy is justifiable. This may, for example, include use by an individual to protect their lawful interests, or by an investigative journalist in the public interest'.[65]

51. OIC notes that in South Australia, the *Surveillance Devices Act 2016* generally prohibits the use, communication or publication of information or material from a listening or optical

[64] See, e.g. Australian Capital Territory, *Parliamentary Debates*, Legislative Assembly, 20 August 1992, 1879–80; Tasmania, *Parliamentary Debates*, Legislative Assembly, 1 May 1991, 935; Victoria, *Parliamentary Debates*, Legislative Council, 5 May 1999, 424 cited in Consultation Paper at [3.156].
[65] Consultation Paper at [3.157].

surveillance device where it is used to protect the lawful interests of a person. There are exceptions to this prohibition:[66]

- A person who was part of the conversation or activity under surveillance may communicate this information or material with another person who was also party to the same conversation.
- Each party to the conversation or activity under surveillance has consented to its use.
- Information is communicated to an officer of an investigating agency for an investigation, action or proceeding.
- Information is used in a relevant action or proceeding.
- A person subjected to violence or an immediate threat of violence uses surveillance to keep evidence of offending.
- Information is communicated to a media organisation.
- Communication is allowed by a court order.

52. A person must seek permission from a judge to use, communicate or publish information or material from a listening or optical surveillance device used in the public interest. A person may communicate the material with the media without a court order. Media organisations are not required to seek a court order.[67]

53. OIC notes the varying approaches in other jurisdictions and considers the approach adopted in South Australia may provide useful guidance in prescribing exceptions to communication or publication prohibitions.

Penalties and remedies

Q – 21 Should prohibited use of a surveillance device or prohibited communication or publication of information obtained through the use of a surveillance device be punishable:

a) as a criminal offence; or
b) by a civil penalty; or
c) as either a criminal offence or a civil penalty, as alternatives?

54. As outlined in the Consultation Paper penalties are generally designed to punish and deter wrongful conduct while civil remedies are generally intended to compensate for the harm caused by the conduct to an individual.

55. It has been the consistent finding of a number of legislative reviews that Australia's privacy regulatory framework does not provide individuals with adequate remedies for invasions of privacy.[68]

[66] Section 9, *Surveillance Devices Act 2016* (SA).
[67] Section 10(1),(2a) or (2(b) *Surveillance Devices Act 2016* (SA).
[68] In its 2008 Report, *For Your Information: Australian Privacy Law and Practice*, the ALRC recommended that federal legislation should provide for a statutory cause of action for serious invasions of privacy. The 2016 New South Wales Legislative's Council Inquiry on *Remedies for the serious invasion of privacy in New South Wales* and the Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010), Ch.7 made similar recommendations.

56. The New South Wales Legislative's Council Inquiry into *Remedies for the serious invasions of privacy in New South Wales* noted that the 'bulk of evidence was that the available civil remedies, in particular the equitable action for breach of confidence, was inaccessible, offered a 'poor fit' and failed to offer appropriate remedy to people who suffered a serious invasion of privacy'.[69]

57. Recently, the ACCC expressed a preliminary view in its inquiry into Digital Platforms that 'deterrence against problematic data practices could be improved by giving individuals the right to bring an action (or class action) against breaches of privacy and data protection regulations'.[70] The ACCC's preliminary recommendations include introducing a statutory tort of serious invasions of privacy (recommendation 10) and giving individuals a direct right to bring an action for breaches of the Privacy Act (recommendation 8(f)).

58. The IP Act allows an individual to make a complaint about an agency's breach of the privacy principles. If an individual – who need not be a Queensland citizen - considers that a Queensland government agency[71] has failed to comply with its obligations under the privacy principles, they are able to make a formal complaint to the agency in the first instance, and to the OIC if they are not satisfied by the agency response.

59. If an accepted complaint cannot be mediated, the complainant can ask OIC to refer the complaint to the Queensland Civil and Administrative Tribunal (**QCAT**) for its determination and orders. QCAT may make an order restraining the agency from repeating any act or practice, order the agency to carry out certain acts, award compensation to the complainant not exceeding $100,000 and/or make further orders against the agency.[72] Payment of a stated amount is to compensate the complainant for loss or damage suffered by the complainant because of the act or practice complained of, including for any injury to the complainant's feelings or humiliation suffered by the complainant.[73] Since enactment of the IP Act, QCAT has made two awards of financial compensation. In both cases, QCAT made an award of $5,000.[74]

60. The Queensland Human Rights Bill 2018 protects 23 human rights, including the right to privacy and reputation. The Bill does not provide for a standalone cause of action allowing an aggrieved person to access remedies, including damages, for any contravention of their statutory human rights under the Bill. The Bill does, however introduce a complaints mechanism, allowing individuals to make a complaint about entities performing public sector functions that are acting in a way that is not consistent with human rights, including the right to privacy and reputation. The broader scope of both this jurisdiction and privacy right would

[69] Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the serious invasion of privacy in New South Wales*, (3 March 2016) at page 9.
[70] Australian Competition and Consumer Commission, *Digital Platforms Inquiry – preliminary report*, December 2018 at page 223.
[71] Including Queensland Government departments, local governments, public universities, hospitals and health services, statutory bodies and other public authorities.
[72] Section 178(a) of the IPA.
[73] Section 178(a)(v) of the IPA.
[74] *PB v WorkCover Pty Ltd* [2018] QCAT 138 concerned the collection and disclosure of an individual's medical records by WorkCover in relation to a worker's compensation claim. *RM v Queensland Police Service* [2017] QCAT 71 considered whether an email about the WorkCover claim of a QPS employee breached (IPP) 4,9,10 or 11.

extend to some private sector entities and surveillance activities not currently subject to privacy regulation in Queensland.

61. OIC notes there are no civil remedy provisions in the surveillance devices legislation of the other Australian states and territories. OIC supports consistency with privacy laws of other jurisdictions.

62. OIC considers that punishment for prohibited use of a surveillance device, or prohibited communication or publication of information obtained through the use of a surveillance device, should reflect the seriousness of the breach, the gravity of the act or intrusion into an individual's privacy and that any proposed penalties or remedies in the legislation are enforceable and accessible. OIC also considers that any proposed penalties should have a deterrence effect.

63. Enactment of surveillance devices legislation in Queensland is unlikely to cover every circumstance where privacy invasions have occurred. Criminal penalties are likely to be reserved from the more serious invasions of privacy. While penalties and remedies (if any) under surveillance legislation will form an important part of the privacy protection framework, gaps will remain. The introduction of a statutory cause of action could serve to 'complement the existing legislative based protections afforded to individuals and address some gaps that exist in both common law and legislation'.[75] A statutory cause of action would necessitate the individual taking action, rather than the regulator.

Q – 28 Should there be an independent regulator and, if so, what entity should this be?

64. As outlined in OIC's response to Q – 1, the use of surveillance devices should be transparent and accountable and subject to rigorous governance and oversight mechanisms. As such, OIC provides in-principle support for an independent regulator.

65. The creation of independent regulators to respond to particular challenges posed by emerging technology is not without precedent in other jurisdictions. For example, the UK office of the Surveillance Camera Commissioner was created under the *Protection of Freedoms Act 2012* to further regulate CCTV.[76] The Biometrics Commissioner was also established by the *Protection of Freedoms Act 2012* to govern the retention and use by the police in England and Wales of DNA samples, DNA profiles and fingerprints.[77]

[75] Office of the Privacy Commissioner, Submission PR 499 [to the ALRC privacy review], 20 December 2007 cited in Australian Law Reform Commission, *For your Information*: *Australian Privacy Law and Practice*, Report No 108 (May 2008) at Report at [74.85].
[76] The role of the Surveillance Camera Commissioner is to encourage compliance with the surveillance camera code of practice: https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about.
[77] https://www.gov.uk/government/news/biometrics-commissioners-fourth-annual-report-2017.

66. The question as to which entity should be the independent regulator is complex and requires careful consideration. A review of existing entities and their functions fails to identity any one entity that represents a natural fit with the functions and powers required to independently regulate surveillance devices legislation in Queensland – noting this will depend on the type and breadth of functions to be performed by an independent regulator For example:

- The regulatory and compliance mechanism of the *Invasion of Privacy Act 1971* is 'primarily criminal, relying on police investigation and prosecution of offences'.[78] OIC is not aware of any prosecutions of offences, to date, under this Act.
- OIC's jurisdiction is limited to protecting people's personal information held by Queensland government entities and does not extend to individuals, the private sector or bodily or other types of privacy. OIC refers complaints not successfully mediated to QCAT for determination, including any compensation.
- The proposed jurisdiction of the Human Rights Commission under the Queensland Human Rights Bill 2018, while establishing statutory protection for the right to privacy, is limited to entities performing public sector functions and forms part of the suite of other administrative law obligations and oversight mechanism that aim to hold the government accountable.[79]
- The Office of Australian Information Commissioner (**OAIC**) regulates the handling of personal information by Australian government entities and all private sector and not-for-profit organisations with a turnover of more than $3million. It does not apply to individuals acting in a private capacity or small businesses.

67. OIC notes suggestions in the Consultation Paper that the functions of existing 'Privacy Commissions' under information privacy legislation could be extended to cover new functions under surveillance devices legislation'.[80] While various law reform commissions[81] have recommended that the Privacy Commissioner in their respective jurisdictions take on the regulator/oversight/awareness role, it is OIC's understanding, that to date, these recommendations have not been implemented. The Consultation Paper acknowledges that, while proposed in some jurisdictions, no Australian jurisdiction includes a specific complaint mechanism in their surveillance legislation.[82]

68. As outlined previously, OIC is an independent statutory body and forms part of the integrity and accountability framework in Queensland. OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor government agency performance, and compliance with, the RTI Act and the IP Act.

[78] Consultation Paper at [3.286].
[79] Explanatory Notes, Human Rights Bill 2018 at page 6 accessed at https://www.legislation.qld.gov.au/view/pdf/bill.first.exp/bill-2018-076.
[80] Consultation Paper at [3.292].
[81] New South Wales Law Reform Commission, *Surveillance: an interim report*, Report No 98 (February 2001) [4.67]; New South Wales Law Reform Commission, *Surveillance*, Report No 108 (May 2005) Rec 2; Victorian Law Reform Commission, Surveillance in Public Places, Report No 18 (June 2010) Rec 9; New Zealand Law Commission, Invasion of Privacy: Penalties and Remedies-Review of the Law of Privacy Stage 3, Report No 113 (January 2010) Rec 18.
[82] Consultation Paper at [3.298].

69. Demand for all OIC services increased in the 2017-18 financial year and this trend continues with external review demand doubling in the past two years. OIC received a record 624 external review applications in 2017-18.[83] The upward trend for external review services, which comprises the largest proportion of our resources, is consistent with other Australian and New Zealand jurisdictions, and may be due to a greater awareness of the right to access. Internationally, the UK Information Commissioner's Office noted demand for independent review of decisions made by public authorities about requests for information continues to increase and expects to receive a record 6,500 cases for consideration in the 2018-19 financial year.[84] Privacy is also frequently in the headlines due to development at the international, national and local level, posing a number of challenges for regulators, including OIC. Due to the unprecedented demand, we are currently monitoring the increased need, and our ability to continue to service the community and agencies and perform our statutory functions consistent with expectations.

70. As noted in the Consultation Paper, the introduction of an independent regulator would involve additional costs, with a potential increase in regulatory burden. The surveillance devices regulatory framework under consideration in this review would represent a significant expansion, and change in nature, of OIC's current jurisdiction.

71. As outlined above, we currently regulate about 230 Queensland larger government agencies, with other very small entities such as boards usually supported by larger agencies. Surveillance legislation may cover individuals and small businesses that are not currently regulated by the Australian or Queensland privacy legislation.[85] In Queensland there are 4,703,193[86] individuals and more than 426,000[87] small businesses. Smart phones, tablets, CCTV, body worn cameras, dash cameras, and other surveillance technology can be operated by any of these individuals, businesses or organisations, including children.

72. The scope of the stakeholders and potential complaints and respondents, is likely to be significantly larger and very different from the group OIC currently deals with. The issues are likely to be more complex. Engagement and communication will require different approaches and greater resources to reach new stakeholder groups, not previously subject to surveillance and privacy regulation.

73. As outlined above, OIC is not in a position to manage any additional demand placed on our services, or expansion of our functions, or nature of those functions. We do not have the necessary powers and enforcement mechanisms to perform the functions of an independent regulator of surveillance devices legislation in Queensland. Unlike the OAIC, OIC does not

[83] Office of the Information Commissioner 2017-18 Annual Report at page 7 accessed at https://www.oic.qld.gov.au/__data/assets/pdf_file/0006/37581/oic-annual-report-2017-18_web.pdf.
[84] Information Commissioner's Office, *Consultation – 'Openness by design' – our draft access to information strategy*, accessed at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-openness-by-design-our-draft-access-to-information-strategy/.
[85] Privacy legislation refers to the IP Act and Australian *Privacy Act 1988*.
[86] Australian Bureau of Statistics, 2016 Census QuickStats, accessed at http://quickstats.censusdata.abs.gov.au/census_services/getproduct/census/2016/quickstat/3?opendocument.
[87] Department of Small Business and Training, *State of Small Business 2018 report*, accessed at https://publications.qld.gov.au/dataset/queensland-state-of-small-business/resource/fc2ff16d-b180-41db-85ae-dc3c100753af

have the power to make a determination about a privacy complaint[88] or seek to enforce a determination in a court.[89] Under the IP Act, OIC is required to refer any complaints unable to be mediated – if asked to do so by the complainant - to QCAT.[90] A significant expansion of OIC's current jurisdiction is also likely to result in increased demand at QCAT. Impacts on demand at QCAT is an important consideration given current resourcing issues.

74. In contrast to the Commonwealth Privacy Act, the IP Act does not currently provide the Information Commissioner with a clear power to investigate an act or practice of his or her own motion where the Commissioner considers that it is desirable that an act or practice be investigated.[91] Own motion investigation powers allow the Commissioner to conduct an investigation without any prior complaint being made. The exercise of 'own motion powers' is beneficial when used in this context as a means of addressing systemic issues. As noted by the ALRC, 'in order to make such investigations effective as a compliance tool, however, it is important that the Commissioner have adequate means to enforce remedies' in the event of a breach'.[92]

75. The IP Act gives the Information Commissioner the power to issue a compliance notice where there has been a serious or a flagrant breach of the obligation to comply with the privacy principles, or a breach, which has occurred five times in the preceding two years. The IP Act sets a high threshold for the issuing of a compliance notice, limiting the range of circumstances in which the Information Commissioner can investigate an act or practice.

76. In its submission to the *2016 Consultation on the Review of the Right to Information Act 2009 and Information Privacy Act 2009*, OIC recommended providing the Privacy Commissioner with an 'own motion power' to investigate an act or practice, whether or not a complaint has been made, to strengthen existing powers in the IP Act to identify any systemic issues arising out of an act or practice of an agency. The Review Report recommended that the IP Act be amended to expressly provide the Information Commissioner with an 'own motion power' to investigate an act or practice, which may be a breach of the privacy principles, whether or not a complaint has been made. Legislative amendments to the IP Act to provide additional powers are a matter for the Queensland Attorney-General and Minister for Justice.[93]

[88] Section 52, *Privacy Act 1988* (Cth).
[89] Section 55A, *Privacy Act 1988* (Cth).
[90] Section 176, IP Act.
[91] Section 40(2) *Privacy Act 1988* (Cth).
[92] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 at [50.14].
[93] Portfolio responsibility for the RTI and IP Acts rests with the Attorney-General and Minister for Justice.

Q – 29 **What regulatory and compliance functions or powers should be conferred on an independent regulator or otherwise provided for under the legislation, for example:**

- **a) conciliation or mediation of complaints about breaches of the legislation;**
- **b) appointment of inspectors to investigate or monitor compliance with the legislation;**
- **c) the issue of compliance notices;**
- **d) starting civil proceedings;**
- **e) education and best practice guidance and advice about the legislation;**
- **f) research, monitoring and reporting of matters relevant to the legislation.**

77. OIC agrees that, in-principle, the regulatory and compliance functions or powers conferred on a regulator should cover the matters listed in (a)-(f). However, as outlined in response to Q – 29, there does not currently exist a regulator in Queensland with functions that align with all of the functions or powers required to effectively regulate surveillance contemplated by the proposed legislated surveillance framework in Queensland.

78. As such, the conferral of functions and powers listed in (a) – (f) will require significant additional resourcing. For OIC to regulate individuals or the private sector would be a fundamental shift in focus requiring significant additional resources and skills. If such functions are allocated without appropriate resourcing, it would undermine the effectiveness of, and community confidence in, a new civil surveillance regime. It would also significantly compromise the community's existing rights to information privacy and access government-held information given the current record demand for OIC services.