QUEENSLAND COUNCIL FOR CIVIL LIBERTIES

Protecting Queenslanders' individual rights and liberties since 1967

Watching Them While They're Watching You

15 February 2019

Mr David Jackson
Queensland Law Reform Commission
PO Box 13312
George Street Post Shop
BRISBANE QLD 4003

By Email: lawreform.commissionjustice.qld.gov.au

Dear Mr Jackson,

RE: REVIEW OF CIVIL SURVEILLANCE AND PRIVACY LAWS IN QUEENSLAND

1. The Queensland QCCL for Civil Liberties **("the QCCL")** is a not-for-profit organisation that exists to protect the individual rights and liberties of Queenslanders.

2. We make this submission in response to your letter dated 20 December 2018 seeking submissions in relation to the review of civil surveillance and privacy laws in Queensland.

Statutory Cause of Action for Serious Invasion of Privacy.

3. Before addressing the specific questions raised in the Consultation Paper, we wish to submit that the Commission should follow the lead of its Victorian counterpart and recommend that the State Parliament enact a statutory cause of action for breach of privacy.

4. We believe that such a measure is necessary to cover any gaps that will inevitably arise in the statutory framework and serve as an important check and balance to the potential misuse of surveillance technology.

5. **We submit that the Commission should** strongly recommend the cause of action recommended by **Australian Law Reform Commission'.**

Scope of a new legislative framework

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

6. Ruth Gavison in her seminal article' argues that privacy is about how we are presented to the world (i.e. what information is known about us), the extent to which we are subject of attention and the extent to which people have physical access to us.

See: Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era,* ALRC Report 123 (2014) 4.1.

PO Box 2281, Brisbane QLD 4001 forum.qccl@gmail.com Enquiries: 0409 574 318

Media Enquiries: Michael Cope, President: 0432 847 154

7. It is our respectful position that privacy underpins human dignity and is fundamentally important to the operation of many human rights, including the rights to association and political opinion. In our view, privacy and the exchange of private (personal or sensitive) information requires trust and steps taken to undermine privacy will also undermine public trust.

8. NA Moreham develops this suggesting that:

> *"In my view, privacy is best defined as the state of "desired in-access" or as "freedom from unwanted access". In other words, a person will be in a state of privacy if he or she is only seen, heard, touched or found out about if, and to the extent that, he or she wants to be seen, heard, touched or found out about. Something is therefore "private" if a person has a desire for privacy in relation to it: a place, event or activity will be "private" if a person wishes to be free from outside access when attending or undertaking it and information will be "private" if the person to whom it relates does not want people to know about ir .*[3]

9. It is trite to say that individual value placed on privacy will vary from individual to individual. The fundamental proposition is that some people will be more concerned about privacy than others but most people will have some aspect of themselves which they wish to keep private.

10. The fundamental proposition is that the law needs to enable individuals to decide for themselves which aspects of themselves they wish to keep private and which they do not. This decision should not be left in the hands of government or private corporations who are at the very best in a situation of a conflict of interest when it comes to these matters and more often than not in fact their interest is served by the reduction in privacy.

11. In our view there is privacy in a crowd. It comes about in two ways that are relevant to a surveillance device, as was explained by our colleagues at the British Columbia Civil Liberties Association in the context of CCTV[4]. A casual glance from a stranger or being photographed by a tourist is different from being surveilled by a surveillance device. The use of a surveillance device involves the user being unobservable by the observed, so there is no possibility of escape or of observing back. The period of observations is almost always much longer or can be than in the case of a person standing in the mall with a camera. The relationship is entirely asymmetric[5].

12. It is our respectful submission that this asymmetric relationship can only be addressed with properly obtaining prior *informed* consent to surveillance and enforceable privacy protections available to the community, including the introduction of a tort for serious invasions of privacy.

13. Furthermore, it is our position that information/data privacy becomes relevant because both public and private bodies of course now have the power to store and analyse by data-matching vast amounts of data[6]. This issue is particularly exemplified by ANPR. While we have no in principle objection to this device, we object to is its use to create new databases. The tool can be perfectly effective in its stated aim of identifying stolen or unregistered vehicles by use of mobile camera with a blacklist, which only records offending vehicles.

14. We also need to be careful not to fall into the trap of diminishing surveillance by private bodies on the basis that they do not have the power of the State. Not only is this distinction not relevant to the concept of privacy advanced here but the recent examples of the metadata and encryption laws'

---

[2] Privacy and the Limits of the Law 89 Yale Law Journal 421.
[3] Privacy in the Common Law: a doctrinal and theoretical analysis 121 LQR 628.
[4] Video surveillance in Public Places https://bccla.org/our_work/video-surveillance-in-public-places/.
[5] See also: Bentham's Panopticon.
[6] See: Queensland Council for Civil Liberties submission to the Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (Submission 10) dated 20 March 2018; Joint Councils for Civil Liberties Submission to the Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018 (Submission 9).

See: Joint Council for Civil Liberties submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* dated 14 October 2018 (Submission 63); Joint Civil Society Submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* dated October 2018 (Submission 55).

show that the state is now passing laws to grant itself access to the data collected by private organisations.

15. The Council specifically rejects the argument that 'If you have nothing to hide, you have nothing to worry about.' In fact, the Council takes the opposite view that 'nobody has nothing to hide' and the 'nothing to fear' rhetoric fundamentally undermines the right to privacy as expressed in the *Universal Declaration of Human Rights* and *International Covenant on Civil and Political Rights.*

16. There are many people who for totally legitimate reasons might want to get lost. For example, the victims of sexual abuse have every reason to change their identities and not be identified. The assertion that the 'innocent have nothing to hide' implies that only those who wish to deceive prize their privacy. In fact, the innocent have plenty of reasons to hide their identity. Some of us visit shops providing electrolysis for hair removal others providing hair transplants, and in neither case do we wish to be recorded doing so by a camera which pans the storefront. Some of us visit drug counselling centres, herbal remedy stores, debt counselling services, a psychiatrist, urologist or a weight loss clinic—all legal pursuits, but not everyone feels comfortable about providing testimonials on TV for them.

17. As the former Victorian Privacy Commissioner noted[8]:

> *"I believe that...anonymity in* a *crowd is dying. It is draining away quickest in crowded places in urban and suburban areas but the trickle has begun in those places.*
>
> *A gradual loss of this aspect of our privacy is a result of several factors which are developing at speed. The consequences for privacy and, more broadly, for other aspects of liberty are very significant depending on the way our society handles this trend."*

18. Borrowing from our British Columbia colleagues we would submit that in order to be acceptable, surveillance of a public place must:

    a. Fulfill an important purpose such as reduction of risk of physical harm or other illegal activities and not simply the control of nuisance such as panhandling;
    b. Not simply drive a problem from one area into another area that does not have surveillance;
    c. Be the least invasive of privacy means of surveillance;
    d. Be advantageous to all or at least to most of the people who are giving up their privacy;
    e. Provide the public with clear notification of its presence in the areas where surveillance occurs, a publicity campaign in the media to inform people of the locales where it is located, etc.,
    f. inform the public of its rationale;
    g. Inform the public about who is monitoring the devices, what use is to be made of the data collected, how long they are to be stored, etc.;
    h. Be monitored by the Information and Privacy Commissioner with respect to its deployment and the use and storage of the data generated;
    i. Clearly achieve what it is meant to achieve;
    j. Not produce data that can be used as part of a data matching program for other than the specific purposes identified in advance. In our view, this must mean that the data is either not collected or is destroyed except for data needed in response to a specific event to be found in the data;
    k. Be more efficient in terms of cost/benefit (in terms of loss of privacy, expense, and effects on other resources on the cost side, and increased security on the benefit side) than alternatives.

[8] The Value of Privacy: A Law Week 2006 Address by Paul Chadwick 23 May 2006

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

19. Different considerations ought to apply to covert surveillance. One of the factors that makes public surveillance unacceptable, is that the watched does not know they are being watched. As the discussion paper notes, the greater the expectation of privacy in a given situation, the less acceptable is covert surveillance.

20. It is our view that anyone undertaking surveillance should be required to notify the public by comprehensible and visible signs.

21. If, however, a person says that notification will impede the effectiveness of the surveillance they should be required to apply to a Court of competent jurisdiction for judicial authority to use the device on a covert basis.

22. Furthermore, in the event that surveillance is covertly targeted to an individual or group of individuals, a judicial warrant ought to issue. Indeed, the European Court of Human Rights has recently affirmed the importance of independent oversight of surveillance tools finding that:

> *"Review and supervision of secret surveillance measures might come into play at three stages: when the surveillance was first ordered, while it was being carried out, or after it had been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictated that not only the surveillance itself but the accompanying review should be effected without the individual's knowledge. Consequently, since the individual would necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it was essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse was potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure"*[9].

23. It is our respectful position that the decision in *Big Brother Watch & Ors -v- The United Kingdom* articulates a correct and accurate position in relation to the operation of surveillance.

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)

24. It is our position that the definition for surveillance device ought to be broadened to include "any technological means to correlating identity data" and identity data ought be broadly defined as "personal information" (as this term is defined at s. 6 of the *Privacy Act 1988* and expressly include information, whether in aggregate or otherwise, that may be used to reasonably identify an individual.

---

[9] European Court of Human Rights, Case of *Big Brother Watch and Others v. the United Kingdom,* Legal Summary, 13 September 2018 *(Applications nos. 58170/13, 62322/14 and 24960/15)* at https://hudoc.echr.coe.int/eng#{"itemid":["0 02-12080"D.

Q-4 If 'yes' to Q-3:

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?

25. We repeat our position that the definition for surveillance device ought to be broadened to include "any technological means to correlating identity data" and identity data ought be broadly defined as "personal information" (as this term is defined at s. 6 of the *Privacy Act 1988* and expressly include information, whether in aggregate or otherwise, that may be used to reasonably identify an individual.

Q-5 Alternatively to Q-3, should new 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?

26. It is our view that the rapidly changing nature of technology requires the use of a technologically neutral definition. We would support the definition including a power to add devices by regulation, but not to remove any device from the definition. The removal of a device should require Parliamentary authorisation.

The use of Surveillance Cameras

Q-6 For what purposes should the use of a surveillance device be prohibited? For example, some or all of:

a. overhearing, recording, monitoring or listening to a relevant conversation;

b. observing, monitoring or recording visually a relevant activity;

c. accessing, tracking, monitoring or recording information <u>that is input into, Qutput from or</u> stored in a computer;

d. determining the geographical location of a person, vehicle or object;

e. some other purpose; for example, the collection of biometric data?

27. It is our submission that this legislation should provide the broadest level of protection. It should extend to the installation, use, maintenance and attachment of a surveillance device. within the meaning of the Act. That should cover all of the purposes listed above.

Q-7 Should the prohibition in Q-6:

(a) **be restricted to intentional or knowing use?**

28. Consistent with our support of a subjectivist approach to the criminal law it is our view that criminal liability should only be imposed for the intentional or knowing use of a device.

(b) **be restricted to private conversations and private activities, or should it extend to some other conversations and activities?**

29. This is of course is the fundamental question. We have already noted our view that privacy does not stop at the door of the house or the office.

30. What is central then is, as is noted in paragraph 3.15 of the discussion paper, is what is meant by privacy. We have already made clear our view that privacy must include some public activities. The use of surveillance devices in public not only implicates information privacy but the other forms of privacy. It will no doubt be argued that information privacy is adequately dealt with by the Privacy Act, both state and Commonwealth. However, it is our view that those Acts are inadequate, particularly the Commonwealth Act which excludes businesses having a turnover of less than $3 million.

31. The current preferred to test for working out if something is private and deserves legal protection is the "reasonable expectation" of privacy test. In the absence of a better test we support it. We accept that it is often criticised as being circular. However, some of those issues are addressed by Moreham's proposals in relations to its formulation.

32. The first problem with the reasonable expectation test is that by focusing on the claimant's reasonable expectations, it suggests that liability depends on whether privacy is likely to be respected in a particular situation, rather than on whether it should be respected in that situation. The consequences of this approach are exemplified by the Supreme Court of California's decision of *Schulman v W Productions Ltd.* In that case, the Court held that a woman did not suffer an actionable breach of privacy when a television filmed her being attended by paramedics at the scene of a serious road accident because she could not have had *"a reasonable expectation that members of the media would be excluded or prevented from photographing the scene"* because *"for journalists to attend and record the scenes of accidents and rescues is in no way unusual or unexpected". In contrast, the court held that the claimant could have an objectively reasonable expectation of privacy inside a rescue helicopter because the court was "aware of no law or custom permitting the press to ride in ambulances or enter hospital rooms during treatment without the patient's consent".* Whether the claimant had an objectively reasonable expectation of privacy therefore depended on whether the media usually respected an individual's privacy in the situations in question.

33. An example of such an application to the interpretation of privacy is the English decision of *Mosley v- News Group Newspwpers*[10]*.*

(c) **extend to attachment installation or maintenance of the device?**

34. We have already expressed our view that the prohibition should extend to this conduct. Of course it's not immediately clear that any of these activities is necessarily less morally culpable than the use of the device. They are all necessary, for some person or another to be able to use the device. On our approach, a person who installed or maintained the device without knowing what it is going to be used for or that it was going to be used unlawfully would not be guilty of an offence in any event. No doubt, to the extent that these activities might be seen as involving a lower level of culpability, which can be reflected in a lower penalty.

Exceptions to the prohibition on the use of a surveillance device

Q-8 In what circumstances should a person be permitted to use a surveillance device with consent? What should be the requirements of consent, and should this vary depending upon the particular use or type of device?

35. On the basis of the approach to privacy taken here, the desire to prevent access for the collection of information is fundamental to the concept. It follows, that any statutory definition must include the

[10] *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB); see also: https://www.thequardian.com/uk/2008/ju1/24/moslev.orivacV.

lack of consent to the access to the person or the collection of the information as an element to be established before a breach of privacy has occurred.

37. However, we do take note of some of the discussion in the Victorian Law Reform Commission report. It is our submission, that the concept of “implied consent“ should not be abandoned. It is a common practice to write off common-law concepts as being too vague or uncertain. It seems to us that there is much law behind the concept and it brings with it a level of flexibility, characteristic of the common law. It seems to us that it would be appropriate to include in the proposed Act a provision to the effect that when considering whether consent is to be implied, two factors should be taken into account:

    a. Whether or not adequate notice has been given of the use of the surveillance device.

    b. Whether or not the person's presence in the particular area where the surveillance device is in use, can truly be considered voluntary.

38. As the discussion paper notes, this raises issues in particular circumstances, namely those who want to install surveillance devices in their home, office, factory or vehicle.

39. The use of surveillance devices in the home is divided into 2 contexts. The first is one that the QCCL has received complaints about people installing cameras trained on their neighbours property. We see no reason why this should be legal. The other is the use of devices in the home. We would say this should only be if there is a warning to visitors. The same applies to factories and offices, so far as they are not intended to monitor employees. We will address that issue in the subsequent consultation.

40. In the case of vehicles we have accepted there is a case for cameras in taxi on the basis of the clear evidence that the project is the safety of drivers. In that case we called for the following safeguards:

    a. access to the photos should be restricted to law-enforcement.

    b. Police should only have access to the photos for the purposes of investigating serious criminal offences against taxi drivers, for all other offences they should have to obtain a warrant.

    c. Real-time surveillance and monitoring should be prohibited.

    d. Used images must be either destroyed within 72 hours unless charges are made.

    e. There should be prominent warning signs in the taxi.

Q-9 Should there be a general exception to the prohibition in Q-6 to permit participant monitoring? Why or why not?

41. There are strong competing considerations on the issue of committing participant monitoring. In particular, as we see it, there is much to be said for the propositions that:

    a. This is commonly practiced as a means of self-protection in commercial, business and domestic contexts.

    b. There is always a risk that a conversation will be recorded in some manner. It may be contemporaneous notes are made either during the course of the conversation or immediately afterwards.

    c. There is a certain level of inconsistency in a situation in which only one means of disclosing the content of the conversation is prohibited.

42. To some extent, these arguments reflect the view of the world developed before the development of the digital world. Modern digital devices have a capacity to record and distribute information which dwarfs the capacity of people to make and distribute written notes of conversations.

43. Development of modern information technology, has put information privacy at the front and centre of peoples' concerns. It is a clear breach of the principal information privacy that a person should be able to record another conversation, without their consent. Note taking, like the tourist taking a photograph in the mall, is an activity which can be seen. The covert recordings of a conversation by a participant in it, is in our view no more different from the covert recording of the conversation by a third party.

44. It is our view that the need to protect a person's interests by use of a recording, could be adequately covered by appropriately drafted exceptions to the rule that conditional upon the introduction of tort for serious invasions of privacy. This will put the focus on the interests which the recording of the conversation is designed to serve and not on the simple fact that the participant has recorded it.

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

45. As noted in our answer to the previous question we do support exceptions to the prohibition on participant monitoring.

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;

46. The QCCL supports the continuation of this exception and submits that it should apply to all devices. It is our view that the decisions of the courts on the existing provision provide an approach that adequately identifies circumstances in which a person's specific interests override the other person's privacy claims.

(b) where it is in the public interest;

47. In general terms, the QCCL does not support public interest exceptions. The term the "public interest" is inherently vague. We would suggest that the history of such exceptions is that they tend to be either under inclusive.

    There is in our submission one public that needs protection – the public interest in a free media there is no doubt, in our submission, that the public interest requires a press which is capable of investigating issues and informing the public about them. This requires them to be able to gather evidence. This must often require them to covertly record conversations. We would submit that the commission should follow the lead of the Australian Law Report Commission and develop a specific exception for responsible journalism with the safeguard of an enforceable remedy for invasion of privacy[11].

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. We take a skeptical approach to health and safety exceptions to privacy law, as they are open to abuse. If there is to be an exception it should be a naturally tailored one like that found in Tasmania which requires that there be, "an imminent threat of serious violence or substantial property damage." We would not support an exception for narcotic offences. We support the further requirement of the Tasmanian statute that the use of the device immediately was necessary.

[11] See for example: *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB).

50. Having said that, it seems to us that on the basis of the decision in *Thomas v Nash,* referred to in the discussion paper, this specific type of exception is not necessary.

(d) where it is not intended to communicate or publish to a person who is not a party?

51. We would not support this exception, for the reasons enunciated by the Victorian Law Reform Commission.

Q-12 Apart from participant monitoring, should there be any exceptions that permit a person to use a surveillance device without consent in particular circumstances?

52. We recognise that there are other interests that should be protected by the availability of surveillance devices and that an enforceable remedy for invasion of privacy serves as a safeguard to these scenarios.

Q-13 If `yes' to Q-12, what should be the particular circumstances for any exceptions and why? For example:

(a) to protect a person's lawful interests;

53. We have considered this above.

(b) where it is in the public interest; or

54. We have already expressed our opposition to public interest exceptions.

(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)?

55. Our comments in relation to the health and safety exception above, apply here.

Q-14 Should there be other circumstances in which the use of a surveillance device is permitted or is not an offence, for example:

(a) for a lawful purpose;

56. We would not support this exception on the basis that it is too vague and open to abuse.

(b) for certain people acting in the course of their occupation, such as media organisations, journalists, private investigators or loss adjusters;

57. We have already noted our support for an exception for responsible journalism.

58. We also recognise, as the New South Wales Reform commission did, that there is a public interest in private investigators or loss adjusters having an exception. There is a clear public interest in the detection and prevention of fraud on insurance. The experience of council members acting as solicitors for both claimants and insurance companies, is that surveillance is an essential tool in this important task. The failure to detect fraud, will only result in increased premiums.

59. In this context, we would support the recommendation of the New South Wales Commission, with the following caveat. That is, that the code of conduct referred to by the commission should be formulated by the Privacy Commissioner and audited by the commissioner on a random basis. These audits should be performed on insurers and of course on the investigators themselves together with an enforceable remedy for invasion of privacy.

(c) to locate or retrieve a device;

60. We would have no objection to this exception on condition that this exception is drafted in a manner that prevents mission or scope creep.

(d) where the use is unintentional; or

61. We have discussed this previously in this submission.

(e) in other prescribed circumstances?

If so, what provision should be made for these circumstances, and why?

62. Firstly, there is the question of monitoring patients. We agree with the Victorian Law Reform Commission, that we need to respect the independence of patients. So that, as that Commission recommended, the correct way to deal with this issue is by appropriate amendments to the *Guardianship and Administration Act.*

63. The next circumstance is tracking objects which are believed to have been stolen. We are thinking of the capacity to track phones such as the "find my iPhone" feature on Apple devices. It may be, on the basis of the decisions referred to in the discussion paper, that the use of this device in those circumstances would not be covered by the current lawful interest exception. If the Commission agrees with that view, then a narrowly drawn exception for such circumstances should be created.

64. We have no objection to an exception for the use of devices in search and rescue operations.

65. We turn to devices to monitor traffic. In this area ANPR is the archetype technology. We have no objection to such a system if it involves the use of a camera with a blacklist, which is used to scan vehicles for those on the blacklist ie stolen, unregistered etc. So that the only information recorded is the location of a vehicle on the list for police action, with the data overwritten in say 72 hours. We oppose any system that is linked to GPS and results in data being added to a database. This position follows from the BCCLA principles set out above, which should be applied to any traffic monitoring system.

Communication or publication of information obtained from a surveillance device

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?

66. It is our position that there should be a general prohibition on the communication or publication **of** dissemination of unlawfully obtained information has the real potential to damage a person's identity, tarnish reputation (in a manner that defamation law is unable to protect or remedy).

67. It is our view that the decision in *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB) articulates the consequence and damage sufferable when unlawfully obtained information is disseminated.

68. We reiterate that a tort for serious invasion of privacy ought to be a key recommendation of the Commission and that such a remedy is overdue in the Australia legal tradition.

Q-16 If 'no' to Q-15, should the communication or publication of information obtained through the unlawful use of a surveillance device be prohibited in particular circumstances, for example, if the communication of publication is not 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 connection with an imminent threat of serious violence or substantial damage to property or the commission of another serious offence;

(e) in the public interest;

(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 use of the device; or

(i) in any other circumstances?

69. It is our position that the only circumstances upon which unlawfully obtained surveillance information may be disseminated is with judicial authority or with the informed consent of the surveillance target.

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?

71. In our view, the appropriate safe guard is an enforceable remedy for invasion of privacy and that, as a general proposition, information ought only be obtained via a surveillance device if the surveillance occurs with informed consent or judicial authority.

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;

(d) to protect the lawful interests of the person making it; 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 use of the device; or

(i) in any other circumstances?

72. We would submit that in the case of product obtained from the lawful use of a surveillance device, the legislation should permit its communication or publication by consent, in the course of legal proceedings, in the performance of a duty and to a person with a reasonable interest in knowing the truth of the matter. The last 2, have parallels in defamation law. Once again, we do not support a public interest exception, and are of the view that the combined exceptions should allow the disclosure of the information in all necessary circumstances. In other words, the combined effect of the exceptions is to reflect the public interest.

Q-19 Should any special provision be made in relation to the communication or publication of information obtained through the prohibited or permitted use of a surveillance device:

(a) by a journalist or media organisation;

(b) by a private investigator;

(c) by a loss adjuster; or

(d) in any other circumstances?

If so, what provision should be made and why?

73. Again, this question requires a case-by-case analysis. For example, in relation to journalism, there is a clear difference between public interest journalism with an underlying quality of journalistic integrity (i.e. surveillance of public servants (including members of parliament) where their conduct brings democracy or the public faith in their ability to responsibly represent an electorate or the performance of their public function) and scandalous journalism intended to vilify individuals.

74. In relation to private investigators and loss adjusters, the communication or publication of information should only be permitted, except to the insurers, where the publication or communication of said information occurs in relation to current or anticipated legal proceedings.

Admissibility of evidence obtained from surveillance device

Q-20 How should the admissibility of evidence, in court proceedings, of information obtained by the unlawful use of a surveillance device be dealt with?

75. It is our position that the admissibility of unlawfully evidence in proceedings requires a careful balance as *"excluding unlawfully obtained evidence may deny trials the most reliable and relevant evidence... admitting it may be seen as legitimizing illicit investigation methods*[12]*".*

76. It is our submission that the decision and discretion to reject evidence must remain with the judiciary with clear legislative guidance that the balance must be between public faith in the administration of justice and on the other the public interest in the protection of an individual for unlawful and unfair treatment. The situation of private individuals can be distinguished from the police, where the current system of discretion vested in judges, fails to provide an adequate deterrence to police officers, since the only penalty they can have inflicted on them for illegally or unfairly, obtaining evidence, is to have that evidence excluded.

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?

77. It is our position that criminal (albeit not exceeding a period of imprisonment of twelve (12) months) and civil remedies ought to apply to prohibited use of a surveillance device or prohibited communication or publication of information obtained through the use of a surveillance device.

78. We additionally consider that injunctive and declaratory relief ought to be available to a plaintiff in civil proceedings.

[12] *Liam Byrne,* 'Admission of evidence obtained in breach of privacy laws' (2007) 78 *Focus on Privacy and FOI.*

79. We further reiterate that the Commission ought to recommend the introduction of a tort for serious invasion of privacy.

Q-22 How should the liability of a corporation, or a corporate officer, for a contravention by the corporation be dealt with?

80. We repeat our response to Question 21.

Q-23 Should there be power to order the forfeiture of a surveillance device used in a contravention of the legislation, or of a report or record of information obtained by the use of a surveillance device in a contravention of the legislation?

81. We consider that it would be appropriate for there to be power to order the forfeiture of a surveillance device used in a contravention of the legislation together with injunctive relief to prevent the ongoing use of similar surveillance devices in circumstances where a surveillance device has been forfeit.

Q-24 Is it necessary for the legislation to include any other ancillary prohibitions, for example, to deal with:

(a) the possession of records obtained from the prohibited use of surveillance devices? (a) the possession, manufacture, supply or advertising of surveillance devices?

(b) the use of surveillance devices to intimidate, harass or hinder a person?

82. We consider that it is appropriate for the legislation to include ancillary prohibitions dealing with the possession of records obtained from the prohibited use of surveillance devices and the manufacture, supply or advertising of unlawful surveillance devices where the possession of records or the manufacture, supply or advertising of unlawful surveillance devices occurs deliberately or with reckless indifference to the legislation.

Q-25 Should there be a right to bring a civil proceeding in respect of a contravention of the prohibited use of a surveillance device or the prohibited communication or publication of information obtained through the use of a surveillance device?

83. We repeat our response to Question 21.

Q-26 If yes to Q-25, what relief should be available to a plaintiff in a civil proceeding, for example:

(a) an order that the contravener is prohibited from conduct (for example, from using a surveillance device) or must do something (for example, remove a surveillance device)?

(b) a declaration (that the conduct was unlawful or that the unlawful conduct breached the person's privacy)?

(c) an order for monetary compensation (for any loss or damage or up to any particular amount)?

(c) other relief?

84. We repeat our response to Question 21.

Q-27 If yes to Q-26(a), should breach of a prohibitory or mandatory order be a criminal offence or dealt with as a contempt or by some other procedure?

85. We submit that a breach of a prohibitory, mandatory or injunctive order ought to be dealt with as contempt.

Enforcement and regulatory powers

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

86. We submit that the Privacy Commissioner and/or Human Rights Commissioner (on the passage of the *Human Rights Bill 2018)* is the appropriate independent regulator.

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 penalty proceedings;

(e) education and best practice guidance and advice about the legislation;

(f) research, monitoring and reporting of matters relevant to the legislation

87. We submit that the above examples are appropriate powers to be conferred on an independent regulator and add emphasis to the importance of education in ensuring that privacy is properly understood on an informed basis and addressed without the need for the cost and resources associated with the Court's intervention.

88. We trust that submission is of assistance and please do not hesitate to contact us should you require any further information or comment.

Yours sincerely,

Michael Cope
President
For and on behalf of the
Queensland QCCL for Civil Liberties

Phone: 0432 847 154

Angus Murray
Vice-President
For and on behalf of the
Queensland QCCL for Civil Liberties

Email: forum.qccl@gmail.com
Phone: 0405 715 427