New South Wales
Council for Civil Liberties

NSWCCL SUBMISSION

ATTORNEY- GENERAL'S DEPARTMENT

PRIVACY ACT REVIEW

ISSUES PAPER

OCTOBER 2020

26 November 2020

About NSW Council for Civil Liberties

NSWCCL is one of Australia's leading human rights and civil liberties organisations, founded in 1963. We are a non-political, non-religious and non-sectarian organisation that champions the rights of all to express their views and beliefs without suppression. We also listen to individual complaints and, through volunteer efforts, attempt to help members of the public with civil liberties problems. We prepare submissions to government, conduct court cases defending infringements of civil liberties, engage regularly in public debates, produce publications, and conduct many other activities.

CCL is a Non-Government Organisation in Special Consultative Status with the Economic and Social Council of the United Nations, by resolution 2006/221 (21 July 2006).

Contact NSW Council for Civil Liberties

http://www.nswccl.org.au
office@nswccl.org.au
Street address: Level 5, 175 Liverpool Street, Sydney, NSW 2000, Australia
Correspondence to: PO Box A1386, Sydney South, NSW 1235
Phone: 02 8090 2952
Fax: 02 8580 4633

Privacy Act Review Issues Paper October 2020

The Council for Civil Liberties (NSWCCL) thanks the Attorney-General's Department for the opportunity to make a submission concerning the Privacy Act Review issues paper.

NSWCCL supports a number of the proposals, outlined in the issues paper, of the ACCC Digital Platforms Inquiry (DPI) and recommendations for reform made by the Australian Law Reform Commission (ALRC).

This submission concentrates on key areas including:

- Definition of personal information,
- Exemptions to the Privacy Act (Act),
- Notice of Collection and consent, and
- A statutory tort.

NSWCCL urges throughout that there be urgent reform of the Privacy Act.

1. Introduction

1.1 The unassailable and unchecked integration of digital technology into everyday life has highlighted the failings of the Privacy Act and necessitates urgent reform of the Act.

1.2 Two main areas of concern in debates about privacy, are the intrusive observance of one's actions and discussion and the misuse of personal information. In terms of the latter this includes especially information that can be used for harassment and prejudiced treatment.

1.3 Privacy is a fundamental human right, in that it is central to the maintenance of democratic societies and is essential to human dignity. In its absence, there is no freedom of expression and information, and no freedom of association.

1.4 Intrusion upon privacy lays the victim open to victimisation and discrimination. Covert intrusions leave a person vulnerable to misinterpretation and mistaken data-matching. The knowledge that words and actions may be being monitored restricts autonomy and hampers personal growth and the development and enjoyment of relationships. In the hands of the unscrupulous, covert surveillance leaves victims open to blackmail.

2. Objectives of the Privacy Act

2.1 The objects of the Act were developed in an environment in which privacy regulation was seen by big business as an obstacle. S2A(b) of the Act states that one of the objects of the act is "to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities". However, privacy, in 2020, is not something to be balanced with commercial or business interests. It is of special importance as it promotes autonomy of the individual and valuable social democratic practices.[1]

[1] Sax, M. (2018) Privacy from an Ethical Perspective *The Handbook of Privacy Studies* [Amsterdam University Press] at 161

2.2 Opting out of digital interactions is not a realistic option for most individuals. Balancing interests therefore amounts to having to agree to terms of access or risking the suffering of economic disadvantage, discrimination or social exclusion.[2]

3. Definition of personal information

3.1 One of the criticisms of the Act is that there is no real definition of privacy. The OAIC has suggested that privacy includes the right to be free from interference and intrusion, to associate freely with whom you want and to be able to control who can see or use information about you.[3]

Such a definition should be considered in this review so that, at least, it can be determined when a practice may be taken to cause privacy harm to an individual.

3.2 The DPI Report recommended that the definition of "personal information" in the Privacy Act be updated "in line with current and likely future technological developments". NSWCCL supports the ACCC recommendation 6(a) that there needs to be greater clarity around the circumstances in which device information may constitute "personal information" under the Act. This would bring Australia in line with international standards.

3.3 NSWCCL supports the updating of the definition of 'personal information' to expressly include inferred personal information. The fact that APP entities may 'find it difficult to practically determine the point at which the inferences they generate become personal information' and that there are borderline cases is not a reason for declining to take action in relation to clear cases.

Combining information collected for different purposes is itself error prone and should be discouraged. See also 6.16 & 6.17

3.4 NSWCCL supports a requirement for 'personal information' to be anonymized, rather than just de-identified for the definition of personal data to not apply. The GDPR provides this protection. Digital platforms, publishers and advertisers often claim to work outside the reach of privacy laws because the data in which they trade is 'de-identified' or 'anonymised' or 'non-personal'. This information can then be used to target individuals. For example, publicly disclosed de-identified data of Melbourne public transport cards could be used to find patterns showing young children travelling without an accompanying adult.[4]

An individual can be differentiated from a dataset and could be tracked, profiled, targeted or otherwise impacted. NSWCCL believes that is a privacy harm which requires greater protection.

---

[2] Lindgren, E.R. (2018) Privacy from an Economic Perspective. *The Handbook of Privacy Studies* [Amsterdam University Press] at 200

[3] Australian Government, Office of the Information Commissioner, What is privacy? https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy/ accessed 26 November 2020

[4] Culnane, C., Rubinstein, B.I.P & Teague, V. (15 August 2019) Two data points enough to spot you in open transport records *Pursuit, The University of Melbourne* https://pursuit.unimelb.edu.au/articles/two-data-points-enough-to-spot-you-in-open-transport-records

4. Exemptions

Small business exemption

4.1 In terms of privacy, small business is virtually unregulated in Australia. For example, with the premise of reducing crime, small businesses are increasingly using CCTV and facial recognition software, capturing movements in and out of shops. This is considered by most Australians as an unreasonable intrusion on their privacy.[5]

4.2 The small business exemption is intended and does reduce regulation around small operators. This means the vast majority of Australian businesses are not legally obliged to comply with standards for fair and safe handling of personal information. This is largely unknown to the Australian public.

4.3 The concept of an exemption based on business size is essentially flawed. How does the public know the turnover of a business and therefore whether or not it is likely to be subject to the law? How can an informed decision be made about using the services of the business?

4.4 The latest intrusive practice, endorsed by government for mandatory use by small business, is the collection of personal data using electronic check-ins (e.g. QR codes). The use of QR codes has not been accompanied by legislation supervising or regulating that use. In NSW, only guidance has been provided and small businesses like restaurants and bars are generally exempt from complying with privacy obligations.[6]

Many businesses have largely opted to outsource their Covid check-in obligations by using free or cheap QR code providers. These platforms are often owned by companies that deal in collecting data, some operating under opaque rules about how that information is stored and used.

4.5 NSWCCL agrees with the ALRC recommendations that the small business exemption be removed.[7] It is redundant.

Employee records exemption

4.6 Privacy in the workplace has been left to federal agencies and the States to regulate under workplace relations legislation but new digital technologies have highlighted the inconsistencies and inadequacies of workplace privacy policy. As outlined in the issues paper, an employee record is a record of personal information relating to the employee and includes sensitive information including genetic information. NSWCCL considers that it may, in certain circumstances, be reasonable to expect employees to object to workplace surveillance, the use of biometrics and the collection of bodily fluids.

---

[5] Leonard, P. (27 Aug 2020) Data privacy in a data and Algorithm enabled world, Gilbert and Tobin https://www.gtlaw.com.au/insights/data-privacy-data-algorithm-enabled-world

[6] Witzleb, N. (11 November 2020) 83% of Australians want tougher privacy laws. Now's your chance to tell the government what you want. *The Conversation* https://theconversation.com/83-of-australians-want-tougher-privacy-laws-nows-your-chance-to-tell-the-government-what-you-want-149535

[7] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, 1358

4.7 Employers must also comply with applicable legislation for occupational health and safety, workplace surveillance, general surveillance and health records legislation, each with specific employer compliance obligations. NSWCCL agrees that consistency in record keeping is desirable and that the removal of this exemption would assist in improving data record practices.

4.8 NSWCCL supports the removal of the employee record exemption.

Political parties exemption

4.9 The exemption for politicians was originally introduced to encourage freedom of political communication. However, a severe lack of privacy is incompatible with political freedom as that freedom presupposes an autonomous, critically evaluating individual. Privacy is a therefore a necessary precondition to freedom of political communication.

4.10 At the time the exemption was introduced, the then Privacy Commissioner argued against the exemption since political institutions "should follow the same practices and principles that are required in the wider community."[8]

As former greens leader Richard Di Natale stated, "... it's really important that we go back, remove those exemptions, ensure that there's some transparency, and allow people to decide whether they think it's appropriate."[9]

4.11 The data environment has significantly changed since the introduction of that exemption and it is no longer appropriate for modern-day online activities.

The exemption permits political parties to intrude on a person's privacy, for example, by targeting with automated call and text messages. This is despite the fact that a majority of Australians believe political parties must abide by the Act in their campaigning activities and voter research databases.[10] Community expectations are that political institutions are subject to privacy constraints.

4.12 The activities of Cambridge Analytica, in which personal information was harvested without authorisation for political targeting, would be likely exempt if it were contracted to an Australian political party.[11]

---

[8] Privacy Commissioner, Malcolm Compton in Vaille, D (22 March 2018) Australia should strengthen its privacy laws and remove exemptions for politicians *The Conversation* https://theconversation.com/australia-should-strengthen-its-privacy-laws-and-remove-exemptions-for-politicians-93717 accessed 12/11/20

[9] In Vaille, ibid

[10] Timothy Pilgrim (then Privacy Commissioner) in Munro K (22 March 2018) Australia's major parties defend privacy exemption over Cambridge Analytica *The Guardian* https://www.theguardian.com/australia-news/2018/mar/22/australias-political-parties-defend-privacy-exemption-in-wake-of-cambridge-analytica accessed 12/11/20

[11] Cadwalladr, C and Graham-Harrison E (18 Mar 2018) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach *The Guardian* https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election accessed 12/11/20

4.13 NSWCCL supports the removal of the exemption. As recommended by the ALRC it should be expressly provided "that the Act would not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication".[12]

4.14 If the ALRC recommendation is not accepted, political parties should at least be subject to the following:

- APP 1, openness and transparent management;
- APP 7, circumstances for disclosure for direct marketing;
- APP 11, security steps;
- APP 12 access;
- APP 13 correction; and
- The requirement to develop information handling guidelines, in consultation with the Commissioner.

Journalism exemption

4.15 Freedom of expression is a fundamental human right, as recognised by article 19 of the ICCPR to which Australia is a signatory. Though implied in the Constitution, freedom of expression has not been implemented in domestic law or by the enactment a statutory Bill of Rights. NSWCCL endorses the enactment of a Bill of Rights.

4.16 Freedom of expression is not absolute however and the law imposes restrictions on certain forms of expression. Community expectations are that the media should respect individual privacy. However, new technologies have brought new non-traditional media and increasingly pervasive forms of journalism.

4.17 NSWCCL supports the ALRC position that the journalist exemption should be retained. However, to balance safety of personal information, a definition of 'journalism' should be introduced limiting the scope of the exemption to acts and practices that are associated with a clear public interest in freedom of expression.[13]

5. Notice of Collection of Personal Information

5.1 Australia is failing when it comes to regulation of Notice provisions. For example, under the current regulatory framework, shopping centre giant, Westfield, does not need shoppers' consent or knowledge to monitor and record them through facial detection by their Smartscreen billboard cameras.[14] Data captured includes the individual's gender, age, demographic markers, location and the time of visit. From this can be determined that

[12] ALRC, For Your Information: Australian Privacy Law and Practice (n 109) at 1433
[13] ALRC Report No 108 Retaining an exemption for journalistic acts and practices
[14] Gillespie, E. (24 Feb 2019) Are you being scanned? How facial recognition technology follows you, even as you shop *The Guardian* https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop

individual's identity.[15] The APPs are complied with because the data collected about shoppers is used for "management and security purposes."

5.2 By contrast, strict GDPR privacy gives citizens the right to control their personal data and be informed about how their information is used. Consent must be clear, provided in an easily accessible form with clear and plain language. The GDPR also states that it must be easy to withdraw consent.

Third party collections

5.3 The OAIC's latest Australian Community Attitudes to Privacy Survey found that 31% of apps requested information not relevant to the app's stated functionality. For example, bluetooth signals emitted by wearable devices can be collected by third parties and in venues such as shopping centres and airports.

5.5 Location data alone can differentiate a dataset, if not lead to the identification of an individual. Community sentiment suggests that location data should be considered highly sensitive and that all location data should be treated as personal information regardless of whether de-identification techniques have already been applied.[16]

5.6 Regulated entities are the custodians of our data and any disclosure of our personal information to third parties and agencies should only occur in very limited circumstances.

6. Consent to collection, use and disclosure of personal information

6.1 NSWCCL does not support the Notice and Consent model used to collect, use and store data in Australia. This model does not encourage meaningful consent by the user.

6.2 The model requires the regulated entity to make a privacy policy available, a more targeted privacy policy at collection of data and seeks consent where necessary.[17] Its purpose is not to inform but to limit the liability of the regulated entity.

6.3 Criticisms of the notice and consent model include:

(a) difficulty for the individual in properly dealing with the scale or to understand the large volume of often complex policies;
(b) perception that there is no real choice especially when a user must use the service;
(c) lack of choice in terms of a range of privacy settings and data minimisation;
(d) data exhaustion; That is, the inability to comprehend or evaluate policies and secondary disclosures.
(e) algorithmic inference and attribute matching.[18]

6.4 The burden of protecting privacy is on the user rather than the preferred alternative of organisational responsibility and accountability. Such an alternative starts from a point of

[15] Vanessa Teague (university of Melbourne) in Gillespie, ibid.
[16] Johnston, A (12 Nov 2020) Location, location, location: online or offline, privacy matters Privacy Law Bulletin 17.6 (September 2020) https://www.salingerprivacy.com.au/2020/11/12/geo-location-blog/
[17] Leonard, op cit
[18] ibid

restricting data flows unless they can be justified within a framework of necessity, proportionality and fairness.

6.5 The power imbalance between consumers and corporations was highlighted in the OAIC's submission to the DPI:

"[C]onsumers may be informed and understand the inherent privacy risks of providing their personal information, but may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative. Further, while 'consent' is only a meaningful and effective privacy self-management tool where the individual actually has a choice and can exercise control over their personal information, studies also show that consumers rarely understand and negotiate terms of use in an online environment".

The OAIC submission suggests a general fairness requirement for the use and disclosure of personal information. The aim is to address the issue of power imbalances between entities and consumers.

6.6 Peter Leonard argues that "Regulators don't require consumers to take responsibility for determining whether a consumer product is fit for purpose and safe… Why should data-driven services be any different?"[19]

6.7 NSWCCL supports a proposal for the Australian Consumer Law (ACL) to be amended so that consent is not sufficient to authorise data practices which would otherwise be unfair, discriminatory or might cause significant harm to an individual.

6.8 The ACL should also include provision for complete no go zones.[20]

Obtaining consent from children

6.9 Children and adolescents need to be offered a necessary and discrete level of privacy to enable them to grow and thrive and develop personal responsibility and autonomy. Much behaviour directed at children should be no go zones.

6.10 Legislation enshrining no go zones would offer a base-level protection, regardless of consent, by identifying and prohibiting collection, use and disclosure practices that are generally considered inappropriate. For example, collecting information to use in targeted advertising to children online.[21]

The role of consent for IoT devices and emerging technologies

6.11 The presence of IoTs in the home and other private and public spaces (e.g.new identifiers such as QR codes) has changed the way that individuals exercise control and security of their

[19] Johnston, A. (29 May2020) Re-thinking transparency: If notice and consent is broken, what now? *Salinger Privacy* https://www.salingerprivacy.com.au/2020/05/29/re-thinking-transparency/
[20] ibid
[21] Australian Government, Office of the Australian Privacy Commissioner (20 November 2019) Privacy implications of the Digital Platforms Inquiry https://www.oaic.gov.au/updates/speeches/privacy-implications-of-the-digital-platforms-inquiry/

information. Individuals cannot exercise meaningful or attainable control over the devices and data that is generated from them. This means that data can be exploited more easily, more easily shared and used for different, unauthorised purposes.[22]

6.12 The collection and use of information from IoTs is suitable for privacy protection and ACL regulation or at least a mandatory (not voluntary) Code of Conduct.

Inferred sensitive information

6.16 The unintended inferences drawn from our personal information is a real threat to privacy. When data is combined from different sources, or taken out of context, or when information is inferred about individuals, notice about likely risks is impossible to deliver and, therefore, informed consent cannot be obtained.[23]

6.17 NSWCCL supports the inclusion of inferred sensitive information in the definition of personal information despite complications with identifying when it starts to be collected. A discussion has to be had as to how to best regulate inferred data, with a focus on transparency and accountability.

7. Statutory tort

7.1 NSWCCL supports the introduction of a statutory tort for serious invasions of privacy to control pervasive civil surveillance and excessive collections of data.

7.2 NSWCCL agrees with the ACCC's recommendation for a statutory tort to the extent that there is a need to address increased exposure to data breach risks, a reduction in trust which could result in consumers avoiding transactions and the potential for particular risk to vulnerable consumers, including children.[24]

7.3 NSWCCL supports the ALRC view that the statutory tort should be contained in a stand-alone Commonwealth Act, to ensure consistency and uniformity, not the Privacy act which deals narrowly with information privacy.[25]

7.4 "The statutory cause of action would relate not only to the privacy of information but also to other types of privacy, such as territorial, communications and bodily privacy."[26] The statutory cause of action should not be subject to the exemptions in the Privacy Act.

7.5 Competing interests, for example, the implied freedom of political communication could be dealt with by including a provision expressly stating that the cause of action does not apply to the extent that it infringes that right.[27]

---

[22] Sax op cit at 165
[23] Johnston op cit
[24] ACCC report op cit
[25] Australian Law Reform Commission, 4. A New Tort in a New Commonwealth Act, serious Invasions of Privacy in the Digital Era (Discussion Paper 80) https://www.alrc.gov.au/wp-content/uploads/2019/08/fr123_4._a_new_tort_in_a_new_commonwealth_act.pdf accessed 16/11/20;
[26] ibid
[27] ibid

This submission was prepared by Michelle Falstein on behalf of the New South Wales Council for Civil Liberties. We hope it is of assistance to the Attorney-General's Department.

Yours sincerely,

Michelle Falstein
Secretary
NSW Council for Civil Liberties

Contact in relation to this submission Michelle Falstein: email michelle.falstein@nswccl.org.au mob 0412980540.