Legal and Legislative Services,

Attorney-General’s Department

GPO Box 464, Adelaide SA 5001

Via email [LLPSubmissions@sa.gov.au](mailto:LLPSubmissions@sa.gov.au)

# November 2021

Dear Legal and Legislative Services

**DRAFT CIVIL LIABILITY (SERIOUS INVASIONS OF PRIVACY) BILL 2021**

We write as members of the [Rights Resource Network SA](https://www.rightsnetworksa.com/) and thank you for the opportunity to provide feedback on the Civil Liability (Serious Invasions of Privacy) Bill 2021  (the Draft Bill). The [Rights Resource Network SA](https://www.rightsnetworksa.com/) is a volunteer-run collaboration that shares information and research among academics, community organisations and individuals who share an interest in protecting the human rights of South Australians.[[1]](#footnote-1) This submission reflects only the views of the authors, but our Network includes a range of experts in privacy law who are also interested in these reforms.

We congratulate the South Australian Government on its commitment to address serious invasions of privacy in South Australia and look forward to working with experts and community members to raise awareness and help address the broad range of circumstances in which individual privacy can invaded, undermined or disproportionately infringed. In this submission we offer our views on how the Draft Bill could be further improved to ensure that it provides holistic protection for invasions of privacy for South Australians. A de-identified Case Study provided by one of the Network members is used to help illustrate some of our key concerns with the respect to the protective scope of the Bill.

**Summary of Recommendations**

We recommend that the Draft Bill be amended to:

1. address scope of the existing limitations and defences contained in section 11 by including ‘proportionality’ criteria modelled on subsection 13(2) of the *Human Rights Act 2019* (Qld).
2. amend the definition of consent contained in proposed section 12 to include a requirement that consent be freely given and informed, based on subsection 6(1) of the *Privacy Act* *1988* (Cth).
3. Remove the subjective test from the assessment of the respondent’s state of mind currently including in proposed subsections s 7(1) and s 7(2) and replace this test objective criteria.
4. Include a clear complaint process for privacy complaints in South Australia, based on Part 6 of the *Information Privacy Act 2014* (ACT).

**Key Features of the Draft Civil Liability (Serous Invasions of Privacy) Bill 2021**

The Draft Bill was introduced following a 2016 Report by the South Australian Law Reform Institute (SALRI) released a report ‘[A statutory tort for invasion of privacy](https://yoursay.sa.gov.au/72219/widgets/351039/documents/214521)’. In the report SALRI concluded that the protections available in South Australia for interferences with a person’s privacy were inadequate and recommended changes to address serious invasions of privacy.

If enacted, the Draft Bill will establish a new cause of action for serious invasions of privacy in South Australia. This proposed new cause of action will offer a remedy for individuals who have had their personal privacy wrongfully invaded, but only if certain criteria are met. For example, the Bill will require the applicant to prove there was a serious intrusion into their privacy or a serious misuse of their private information. This could include a physical intrusion into private space, watching, listening to, photographing or recording private activities, or obtaining, disclosing or disseminating private information. The application also needs to show that:

* there was a reasonable expectation of privacy
* the invasion of privacy was serious
* the conduct was undertaken intentionally.

A number of individuals and organisations will fall outside of the scope of the proposed new cause of action, including journalists, or those invading the privacy of another in circumstances where the ‘public interest in the matter that outweighs the individual’s privacy’. There are also range of defences available to a defendant, modelled on the defences available in defamation law.

**Rights Enhancing Features of the Draft Bill**

This Bill promotes the internationally recognised right to privacy which is a positive and welcome step forward for rights protection in South Australia. The right to privacy is protected at the international level. For example, Article 17 of the International Covenant for Civil and Political Rights provides:

1. No one shall be subjected to arbitrary or unlawful interference with his [sic] privacy, family, home or correspondence, nor to unlawful attacks on his [sic] honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.[[2]](#footnote-2)

By creating a new cause of action for serious invasions of privacy, the Draft Bill helps give meaning to this internationally recognised right and provides remedies for breaches of this right in certain circumstances. By including some key principles around the concept of privacy, the Draft Bill also has the potential to add clarity and certainty to an otherwise uncertain and context legal landscape in South Australia when it comes to personal information and privacy in a range of settings (see below description of current South Australian law).

The Draft Bill also has the potential to engage South Australian courts and lawmakers in a process of balancing rights that is familiar to human rights law for example proposed section 11 of the Bill provides:

11—Countervailing public interest (1) An individual does not have an action on a statutory cause of action if a countervailing public interest balances with or outweighs the public interest in upholding the privacy of the individual.

However, as noted below, this balancing exercise lacks some of the key features of human rights-based approaches to proportionately which we suggest should be included to improve the rights enhancing quality of the proposed new law.

**Potential Rights Concerns with the Draft Bill**

1. *Insufficient scope of protections – width and breadth of limitations and defences*

Despite the rights-enhancing objects of the Draft Bill, the effectiveness of the statutory cause of action is undermined by the width of available exclusions,[[3]](#footnote-3) particularly those limitations that relate to the handling of personal information by Government.[[4]](#footnote-4)  The Draft Bill recognises that the right to privacy can and should be limited to balance other important ‘countervailing’ rights and interests (such as freedom of expression) with the right to privacy. This is in line with the approach at international law, which recognises that the rights contained in Article 17 can be limited if necessary to protect or promote other individual human rights, provided the limitation is proportionate. However as currently drafted, these countervailing public interest provisions are potentially disproportionately broad in scope. For example, proposed section 11 of the Draft Bill provides:

1) An individual does not have an action on a statutory cause of action if a countervailing public interest balances with or outweighs the public interest in upholding the privacy of the individual.

(2) For the purposes of subsection (1), a court may, for example, consider the following countervailing public interest matters:

(a) freedom of expression, including political communication and artistic expression;

(b) the proper administration of Government;

(c) open and transparent justice;

(d) public health and safety and scientific advancement;

(e) national security;

(f) law enforcement and the detection of crime and fraud

This places excessive emphasis on the ‘countervailing’ public interest, which is further highlighted by the wide, non-exhaustive list of countervailing public interest matters in proposed section 11(2). Importantly, many of these extend to government entities which pose one of the biggest risks for individuals concerned about their privacy and personal information.[[5]](#footnote-5) The recent complaints surrounding use and retention of individual information provided through QR codes and contact tracing[[6]](#footnote-6) would not be actionable based on proposed section 11. The proper administration of government (proposed section 11(2)(b)) and the public health and safety (proposed section 11(2)(d)) would exempt this information from the statutory cause of action. In circumstances where SAPOL, the Chief Health Officer and the government generally already has a wide range of power and discretion under the *South Australian Public Health Act 2011* (SA), *Emergency Management Act 2004* (SA) and other similar legislation, these wide exclusions undermine public confidence in the government and may lead to individual mistrust of government use of information, affecting individual willingness to comply with directives and undermining the effective management of the pandemic.[[7]](#footnote-7)

This could extend further to pose issues for an individual where a ‘countervailing public interest’ may compromise sensitive personal information for example in the case study below, the school’s need to maintain up-to-date contact records of parents and caregivers could be a ‘countervailing public interest’ which places a parent at risk of being exposed to domestic violence.

The width of defences may also significantly hinder the effectiveness of the statutory cause of action: for example, an excessively wide definition of ‘proceedings of public concern’ for the defence of fair report of proceedings in public concern in proposed section 17. This is further undermined by the high standard required for the applicant to defeat the defence in proposed section 17(2): ‘…if, and only if, the applicant proves that the information was not published or disclosed honestly for the information of the public or the advancement of education.’

There is also a general defence of lawful authority contained in proposed section 13 which limits the extent to which government agencies, including law enforcement agencies and service delivery agencies, are bound by the protective provisions of the Draft Bill. Proposed section 10 (4) also excludes ‘the conduct of a person in prescribed circumstances’ from the scope of the cause of action. This could mean the responsible Minister could list certain public officers or departments who are exempt via regulation.

**Case study – The Need for Robust Privacy Protections in South Australia**

An Adelaide mother enrolled their child at a local Catholic primary school to commence in 2019.  The mother attended the enrolment interview with her child, where she submitted a completed enrolment form, containing sensitive and personal information about the mother, (as is required by the school and State legislation).  At that time the mother told the staff member not to disclose any written information provided by the mother ever, to the child’s father.  The staff member agreed to this.

A couple of weeks after this the mother started to receive hang up phone calls.  After contacting the school, she was told, that the enrolment form had been emailed in its entirety to the father.  The mother subsequently had to change her phone number and email.  She also found it difficult to find anyone willing to be an emergency contact for her child with the school.

After making a complaint to the Principal, the mother continued to receive child contact details paperwork annually for the purpose of confirming and updating details.  Critically, these forms contain all the details of her child’s emergency contact people, who are friends of the mother and all of the father’s private information.  These are further breaches and indicate that the father may also be continuing to receive the mother’s details.

Currently, when this type of privacy breach occurs in South Australia, there is limited access to any effective legal remedy, despite the breach potentially exposing victims of domestic violence and their children to increased risk. There is no clear complaints process, other than to repeatedly contact the School, where the mother could face a power imbalance or other barriers to having her complaint addressed. Where complaints are made to other federal or state privacy bodies, often the response is circular, where the victim is requested to contact the school again before the other agency will engage with her complaint.

This Case Study raises the question of whether the Draft Bill would provide an effective remedy for the mother in this scenario.

A number of threshold tests would appear to be met. For example, there was a reasonable expectation of privacy, and a serious breach of privacy by disseminating enrolment contact details to other parties by email that exposed the mother and child to potential risk of harm.

However, there are concerns that as currently drafted the victim in this scenario may not be able to access the proposed new cause of action contained in the Draft Bill due to the breadth and width of the proposed limitations and defences described above.

In order to address the potentially disproportionately broad scope of the existing limitations and defences whilst at the same time continuing to recognize the need to balance the right to privacy with other important public interests such as freedom of expression, the Queensland *Human Rights Act 2019* (Qld) could provide a pathway forward. This legislation protects the right to privacy (in section 25) but also recognises that the right can be subject to ‘reasonable limits’, for example where no other less restrictive means are reasonably available to preserve the other important public interest or right. It provides guidance to decision makers who are tasked with determining the scope of these ‘reasonable limits’ explaining in subsection 13(2) that:

(2) In deciding whether a limit on a human right is reasonable and justifiable … , the following factors may be relevant—

(a)the nature of the human right;

(b)the nature of the purpose of the limitation, including whether it is consistent with a free and democratic society based on human dignity, equality and freedom;

(c)the relationship between the limitation and its purpose, including whether the limitation helps to achieve the purpose;

(d)whether there are any less restrictive and reasonably available ways to achieve the purpose;

(e)the importance of the purpose of the limitation;

(f)the importance of preserving the human right, taking into account the nature and extent of the limitation on the human right;

(g)the balance between the matters mentioned in paragraphs (e) and (f).

Including this type of provision within the Draft Bill, for example with respect to the limitation provision currently contained in proposed section 11, could help address some of the concerns outlined above.

1. *Limited definition of consent*

Proposed section 12 provides a defence of consent to the statutory cause of action. The term ‘consent’ is defined in proposed section 12(2) as ‘express consent or implied consent’. This definition – which is designed to exclude the protective clauses in circumstances where an individual agrees to sharing their personal information or otherwise relinquishing their right to privacy - is missing several key features of standard legal conceptions of *free and informed* consent. As currently drafted it has the potential to undermine the right-enhancing features of the Draft Bill and could be open to misuse.

Adopting a revised definition of consent that includes the requirement that consent be *freely made* and *informed* would remedy this deficit and align with both the Australian Law Reform Commission (ALRC) and South Australian Law Reform Institute (SALRI) recommendations,[[8]](#footnote-8) and the Australian Privacy Principles.[[9]](#footnote-9) The ALRC Report specifically refers to consent being freely given (not obtained by duress) and clearly relating to the contravention/conduct in question.[[10]](#footnote-10) The SALRI recommendation supports this definition.[[11]](#footnote-11)

The *Privacy Act 1988* (Cth) adopts the same definition of consent as the proposed Bill,[[12]](#footnote-12) but the APPs go further than this and provide the four key elements of consent in Chapter B.35:

‘The four key elements of consent are:

* the individual is adequately informed before giving consent
* the individual gives consent voluntarily
* the consent is current and specific, and
* the individual has the capacity to understand and communicate their consent’

B.36-B.58 discusses these elements in depth, including an explanation of how consent is obtained, when consent will be impaired by duress, coercion or pressure, whether an individual has a ‘reasonable opportunity’ to provide consent and capacity to consent.

The Draft Bill would benefit from a more comprehensive definition of consent which could draw on the APPs for consistency and clarity.

1. *Focus on subjectivity*

Several aspects of the Draft Bill focus on a subjective consideration of the state of mind of the respondent to an action of serious invasion of privacy, which have the potential to undermine the rights-enhancing impact of the other provisions. For example, proposed subsection 7(2)(b) refers to ‘the *state of mind* of the respondent’ when assessing whether a contravention is serious. This is a contrast to proposed subsection 7(2)(a) which refers to an objective assessment of the applicant: ‘the degree of offence, distress or harm to dignity likely to be caused to*a person of ordinary sensibilities* in the position of the applicant…’

While this is consistent with SALRI recommendations,[[13]](#footnote-13) it may pose difficulties for judges required to assess ‘whether the respondent was acting with *malicious intent’* under proposed subclause 7(2)(b)(i) or ‘whether the respondent *knew* the invasion of privacy was likely to offend, distress or harm…’ due to the fact that these elements of intent and knowledge are qualified by the *state of mind* of the respondent.

Proposed subclause 7(1)(c) refers to the respondent engaging in conduct ‘*intending* to intrude’ and ‘*being aware* of material risk of intrusion’. However, in proposed subclause 7(1)(c) ‘intention’ and ‘awareness’ (which must be proven by the applicant) are not qualified by any subjective or objective criteria. Both the assessment in proposed subsections 7(1) and 7(2) should be based on objective criteria.

By comparison, the ACT legislation simply refers to ‘an interference with an individual’s privacy’ as being a breach of a Territory Privacy Principle (TPP)[[14]](#footnote-14) which is modelled similarly to the federal APPs.

The defence of necessity in proposed section 14 similarly employs a subjective test (what the respondent genuinely believedto be necessary). The assessment of proportionality is also based on ‘the circumstances as the respondent believed them to be, reasonably proportionate to the threat or risk that the respondent genuinely believed to exist.’

Proposed subsection 14(2) which provides an exhaustive list of ‘defensive purposes’ does not assist with the assessment of a respondent’s genuine belief: a respondent may hold a genuine belief as to a defensive purpose even in a situation where this is completely unreasonable. For example, a business owner may think it is appropriate to disclose the personal details of an individual customer who was rude to them on their website. Another example could be a disgruntled neighbour posting pictures, address and other details relating to their neighbours on social media because the neighbours are being too loud at night. The respondent in this situation holds a ‘genuine belief’ that their conduct is justified, even though it is objectively unreasonable.

The protective capacity of the Draft Bill could be enhanced by incorporating objective criteria when assessing the respondent’s intention, knowledge, awareness etc. This would strike a better balance between the right to privacy and the need to preserve other public interests including procedural fairness to the respondent. The cause of action in proposed section 7 and the defence of necessity in proposed section 14 should assess the reasonableness of the respondent’s actions based on objective criteria for example how a reasonable person in the respondent’s position would have acted in the circumstances.

1. *Lack of clear complaint process*

Proposed section 5 of the Draft Bill outlines that the appropriate jurisdiction for an action is either the Magistrates or District Court depending on the amount claimed by the applicant. While this is an appropriate forum for ultimate resolution of legal disputes between private parties, the most significant public concerns relating to breaches of privacy derive from the handling or mishandling of personal information by government bodies.[[15]](#footnote-15) For this reason, it is necessary for applicants to have recourse to some kind of statutory body or authority for reporting of breaches of privacy by government agencies or public servants. Such a complaints body would also provide an important preventative and educative purpose, and address the current confusion surrounding the range of different laws and guidelines governing the use, sharing and disclosure of personal information by government agencies and officers in South Australia.[[16]](#footnote-16) A complaints body could, for example, publish accessing information about existing laws and standards, and help individuals to understand when and why their personal information is being collected, accessed or shared. It could help local governments or other public bodies who are trying to protect and promote the right to privacy to develop and implement robust privacy policies. It could also provide independent Privacy Impact Assessments for proposed new laws or policies, which would provide a valuable evidence base for government, parliament and the public to assess the merits of employing new technologies such as facial recognition technologies in their operations.

This could be in the form of a SA-based Information Commissioner or similar authority.[[17]](#footnote-17) The case study above highlights the need for victims or applicants to have a clear, accessible and effective process for making complaints that has jurisdiction to consider complaints against South Australian agencies and departments.

The ACT legislation offers a model for how such a complaints system can be established, with benefits for both potential applicants and government officers and agencies. Under the ACT model an individual first makes a complaint to the ‘information privacy commissioner’,[[18]](#footnote-18) who must provide appropriate assistance to the individual (for example, by advising the individual about the complaint process or helping the individual to put a privacy complaint in writing).[[19]](#footnote-19) The commissioner must then inform the respondent about the complaint,[[20]](#footnote-20) before ‘dealing’ with the complaint.[[21]](#footnote-21) After review, if the commissioner is satisfied that there has been an interference with privacy, the commissioner then informs the parties that the complainant may apply for a court order.[[22]](#footnote-22) This process is far more user-friendly and provides guidance to the individual complainants rather than sending them directly to court proceedings. The commissioner’s functions also extend to promoting an understanding of the TPPs generally and assisting public sector agencies to comply with the TPPs,[[23]](#footnote-23) fostering a proactive approach to prevent interferences with individual privacy rather than just reacting to breaches when they have occurred.

**Broader Legal Context**

*Federal Privacy Law*

It is important to note as a starting point that there is no standalone right to privacy at the federal level in Australia,[[24]](#footnote-24) although there are a range of legislative and regulatory protections that operate to limit the use, disclosure and sharing of personal information in certain contexts. For example, at the federal level, the *Privacy Act 1988* (Cth) (‘the Privacy Act’) governs how personal information is handled by federal government agencies and any organisation with an annual turnover of more than $3 million.[[25]](#footnote-25) The Office of the Australian Information Commissioner (‘OAIC’) is the independent national regulator for privacy and freedom of information in matters relating to federal government agencies.[[26]](#footnote-26)Examples of federal agencies include the Australian Taxation Office, the Department of Defence, the Department of Home Affairs and the Department of Human Services.[[27]](#footnote-27)

The use of personal information by state government agencies is governed by state legislation and other instruments and overseen by state-based privacy committees or information commissioners (OAIC n.d.-a). In NSW, Victoria and the ACT, privacy laws relating to the use of health information apply to both the public and private sector,[[28]](#footnote-28) whereas Queensland, the Northern Territory and Tasmania have privacy laws that only apply to public sector health service providers.[[29]](#footnote-29) In Victoria, ACT and Queensland where human rights legislation is in force, there is also a human rights framework for assessing the privacy impact of laws and policies and for handling privacy complaints.[[30]](#footnote-30) Western Australia and South Australia do not have legislation specifically concerning privacy, however avenues for complaints relating to health services and privacy still exist in these jurisdictions. In South Australia, privacy complaints relating to state departments, for example the Department for Correctional Services, the South Australian Housing Authority, the Department for Child Protection, are handled by the Privacy Committee of South Australia (‘the Privacy Committee’).

As noted by the Australian Law Reform Commission (‘ALRC”) in *For Your Information: Australian Privacy Law and Practice*, even in jurisdictions where the ‘right to privacy’ is protected or acknowledged in law, this right is not absolute (ALRC 2008, p. 104).The right to personal privacy involves a balance of competing rights and interests (ALRC 2008, p. 104), including public health, which the National Health and Medical Research Council describes as a balance between the public interest in protecting individual privacy and the public interest in using that information for the benefit of others (National Health and Medical Research Council 2004, p. vii).

## Current law in South Australia

In South Australia there is no Privacy Act or Human Rights Act and no privacy commissioner to make a complaint to, however South Australian public agencies must still account for the way they handle personal information by complying with the Privacy Principles and special Cabinet directives about the handling of personal information. This includes Cabinet Administrative Instruction 1/89 which explains that personal information should not be used except for a ‘purpose to which it is relevant’ and should not be shared with other agencies unless a range of criteria apply, which includes the consent of the owner of the information but also if the disclosure is ‘reasonably necessary for the enforcement of the criminal law’ or if ‘the person disclosing the information believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious threat to the life, health or safety of the record-subject or of some other person’.[[31]](#footnote-31)

The use of personal information in South Australia is governed by a range of federal and state legislation, policies and Cabinet directives. Working out which law applies in which circumstance can be complex and opaque. This makes it difficult for individuals to access clear information and know what their rights are when it comes to the use, disclosure or correction of personal information, and the options available to them if they think that their personal information has been misused. This is exacerbated in the South Australian context, where there is no central body (such as an Information Commissioner) tasked with providing information about how personal information should be used or protected in different contexts.

The handling of personal information by South Australian government agencies is governed by the Privacy Principles.[[32]](#footnote-32) Part 2 of the Privacy Principles govern the collection, storage, access, use, correction and disclosure of personal information with which South Australian public sector agencies must comply.[[33]](#footnote-33) Similar principles also apply in other Australian States and Territories (eg Territory Privacy Principles (ACT); Patient Confidentiality Policy (WA), Personal information protection principles (Tas) ), with some jurisdictions such as the ACT, NSW and Tasmania codifying these principles into legislation (*Privacy and Personal Information Protection Act 1998* (NSW);  *Information Privacy Act 2014* (ACT); *Personal Information Protection Act 2004* (Tas)).

The Privacy Principles apply to the handling of personal information by government agencies such as SA Health. Each of these agencies are in turn governed by different pieces of legislation. For example, privacy in relation to people’s health care in South Australia is also governed by health legislation and regulations, namely the *South Australian Public Health Act 2011* (SA) (‘Public Health Act’), the *Health Care Act 2008* (SA) (‘Health Care Act’) and the *Mental Health Act 2009* (SA) (‘Mental Health Act’). For example, the Public Health Act lists a patient’s right ‘to have his or her privacy respected and to have the benefit of patient confidentiality’ as one of its key principles, albeit subject to the ‘overriding principle is that members of the community have a right to be protected from a person whose infectious state or whose behaviour may present a risk, or an increased risk, of the transmission of a controlled notifiable condition’.[[34]](#footnote-34) The use of and access to personal information and medical information is also regulated by the *Emergency Management Act 2004* (SA) during a declared emergency.[[35]](#footnote-35)

Public sector agencies in South Australia must not collect information from individuals by unlawful or unfair means, nor should it be collected unnecessarily.[[36]](#footnote-36) The collection of information includes ‘gathering, recording or acquiring information from any source and by any means’ (see eg. SA Health 2019a, p. 8). For collection to be lawful, the record-subject must be told, unless it is obvious, before collection, or as soon as is reasonably practical after collection, the purpose for which information is being collected.[[37]](#footnote-37) This is the ‘purpose of collection’.[[38]](#footnote-38) In the health context, for example, the dominant purpose for which personal information is collected is the ‘primary purpose’ though this term is broadly understood to mean the provision of care or an episode of care (SA health 2019a, p. 8). The person about whom the information relates must be told if the collection of information is authorised or required by law and be told in general terms about the usual practices with regard to disclosure of the personal information.[[39]](#footnote-39) Agencies are under an obligation to ensure personal information collected is accurate and up to date, and may not collect information that is irrelevant or excessively personal.[[40]](#footnote-40) However, despite these guidelines, many South Australian agencies are given broad powers to request or access personal information if necessary to enable them to fulfill their statutory functions. In the health context, for example, this includes furnish such information as is reasonably required’[[41]](#footnote-41) for the purposes of the Act, which include the collection of information about ‘incidence and prevalence of diseases and other risks to health in South Australia for research or public health purposes’.[[42]](#footnote-42) These powers have been invoked and broadened in the context of the South Australian response to the COVID-19 pandemic, and with the activation of emergency management legislation giving rise to new questions and concerns about the extent to which the right to privacy is adequately protected under South Australian law.

**Conclusion**

Due the challenges associated with implementing holistic protections against invasions of privacy in South Australia, we consider this Bill to be an important positive step in the right direct, particularly if the changes recommended above are implemented. We also wish offer to help facilitate further community consultation on this important reform. In our view, the South Australian community is eager and well placed to assist in the development of more holistic privacy protections and for this reason the Rights Resource Network SA is preparing to host a community forum on the topic in early 2022. We look forward to speaking to you further about this important area of law reform. Please be in touch with on sarah.moulds@unisa.edu.au to arrange a meeting with the relevant members of the Rights Resource Network SA.

Yours sincerely

Dr Sarah Moulds,

Director, Rights Resource Network SA

Anja Pich

Lecturer in Law, University of South Australia

Stephanie Wood

Member, Rights Resource Network SA

1. The Rights Resource Network is a volunteer-run network that received funding from the Law Foundation of South Australia in 2020 and 2021. It exists to share information and create opportunities for collaboration and joint advocacy among academics, community organisations and individuals who are committed to protecting the human rights of South Australians. The Network is governed by a volunteer Advisory Group with broad range of expertise and experiences. For more information visit <https://www.rightsnetworksa.com/> [↑](#footnote-ref-1)
2. International Covenant for Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). [↑](#footnote-ref-2)
3. Compare, for example, *Information Privacy Act 2014* (ACT) which has a much wider scope of operation and is not limited by exclusions and defences. *Information Privacy Act 2014* (ACT) s 19 ‘permitted general situation’ covers some defences (eg where it is unreasonable to obtain the individual’s consent) but has a much narrower scope than the proposed SA Bill. Similarly, s 25 covers some exemptions but again much narrower scope than SA Bill. [↑](#footnote-ref-3)
4. Sarah Moulds [Four ways to rebuild trust in our chaotic state parliament - InDaily](https://indaily.com.au/opinion/2021/10/15/four-ways-to-rebuild-trust-in-our-chaotic-state-parliament/); [Personal privacy versus public health in a pandemic - InDaily](https://indaily.com.au/opinion/2020/11/24/personal-privacy-versus-public-health-in-a-pandemic/) [↑](#footnote-ref-4)
5. See eg Queensland Crime and Corruption Commission, *Operation Impala – Report on Misuse of Confidential Information in the Queensland Public Sector* (Report, February 2020): recommends a new criminal offence for misuse of confidential information by public sector employees <<https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf>>; Information and Privacy Commission NSW, *Data Breach Guidance for NSW Agencies* (Report, September 2020): examples of public sector data breaches <<https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies>>; cf *Information Privacy Act 2014* (ACT) s 20: ‘ a public sector agency must not do an act, or engage in a practice, that breaches a TPP’. [↑](#footnote-ref-5)
6. Isabel Dayman, ‘SA Health Holding QR Code Check-in Data Indefinitely, Report Finds, as Risk of Breach Revealed’, *ABC News* (online, 12 October 2021) <<https://www.abc.net.au/news/2021-10-12/sa-qr-check-in-data-audit/100533790>>; Law Society of South Australia, ‘Privacy & QR Codes: How do we Keep our Personal Data Safe?’, (online, 1 February 2021); <<https://www.lawsocietysa.asn.au/Public/Publications/Resources/PRIVACY___QR_CODES__HOW_DO_WE_KEEP_OUR_PERSONAL_DATA_SAFE_.aspx>>. [↑](#footnote-ref-6)
7. Sarah Moulds, ‘Personal Privacy versus Public Health in a Pandemic’, *InDaily* (online, 24 November 2020) <<https://indaily.com.au/opinion/2020/11/24/personal-privacy-versus-public-health-in-a-pandemic/>>. [↑](#footnote-ref-7)
8. Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Final Report No 123 (2014) 198 [11.61] (‘ALRC 2014 Report’); South Australian Law Reform Institute, A Statutory Tort for Invasion of Privacy, Final Report 4 (2016) Recommendation 16 (‘SALRI 2016 Report’). [↑](#footnote-ref-8)
9. *Privacy Act 1988* (Cth) sch 1. APP Guidelines Chapter B.35: <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts#consent> [↑](#footnote-ref-9)
10. ALRC 2014 Report [11.61]. [↑](#footnote-ref-10)
11. SALRI 2016 Report, Recommendation 16. [↑](#footnote-ref-11)
12. *Privacy Act* (n 3) s 6(1). [↑](#footnote-ref-12)
13. SALRI 2016 Report, Recommendation 9. [↑](#footnote-ref-13)
14. *Information Privacy Act 2014* (ACT) sch 1. See also *Information Privacy Act 2009* (Qld) Ch 2; *Privacy and Personal Information Protection Act 1998* (NSW) Pt 2. [↑](#footnote-ref-14)
15. See eg Australian Law Reform Commission, Serious Invasion of Privacy in the Digital Era, Final Report No 123 (2014) 198 [11.61] (‘ALRC 2014 Report’); Isabel Dayman, ‘SA Health Holding QR Code Check-in Data Indefinitely, Report Finds, as Risk of Breach Revealed’, *ABC News* (online, 12 October 2021) <<https://www.abc.net.au/news/2021-10-12/sa-qr-check-in-data-audit/100533790>>; Law Society of South Australia, ‘Privacy & QR Codes: How do we Keep our Personal Data Safe?’, (online, 1 February 2021); <<https://www.lawsocietysa.asn.au/Public/Publications/Resources/PRIVACY___QR_CODES__HOW_DO_WE_KEEP_OUR_PERSONAL_DATA_SAFE_.aspx>>. [↑](#footnote-ref-15)
16. See for example the federal Office of the Australian Information Commissioner website <https://www.oaic.gov.au/>. [↑](#footnote-ref-16)
17. SA does not have a State-based privacy commissioner: SA Privacy Committee is limited to complaints regarding State departments. [↑](#footnote-ref-17)
18. See also NSW Information and Privacy Commission under *Privacy and Personal Information Protection Act 1998* (NSW) Pt 4; *Privacy Commissioner under Information Privacy Act 2009* (Qld) Pt 4. [↑](#footnote-ref-18)
19. *Information Privacy Act 2014* (n 8) s 6(3). [↑](#footnote-ref-19)
20. Ibid s 37. [↑](#footnote-ref-20)
21. Ibid Div 6.3. [↑](#footnote-ref-21)
22. Ibid s 45. [↑](#footnote-ref-22)
23. Ibid s 29. [↑](#footnote-ref-23)
24. The right to privacy is protected at the international level. See, eg, Article 17 of the *International Covenant for Civil and Political Rights* which provides: ‘1. No one shall be subjected to arbitrary or unlawful interference with his [sic] privacy, family, home or correspondence, nor to unlawful attacks on his [sic] honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks’: *International Covenant for Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). [↑](#footnote-ref-24)
25. *Privacy Act 1988* (Cth) ss 6C-6F. [↑](#footnote-ref-25)
26. <https://www.oaic.gov.au/> [↑](#footnote-ref-26)
27. For a list of federal government departments and agencies see: <https://www.directory.gov.au/departments-and-agencies>. [↑](#footnote-ref-27)
28. For example *Health Records and Information Privacy Act 2002 No 71* (NSW) s 11; *Health Records Act 2001* (Vic) s 1; *Health Records (Privacy and Access) Act 1997* (ACT) s 4. [↑](#footnote-ref-28)
29. For example [*Information Privacy Act 2009* (Qld)](https://www.legislation.qld.gov.au/view/html/inforce/current/act-2009-014); [*Information Act 2002* (NT)](https://legislation.nt.gov.au/en/Legislation/INFORMATION-ACT-2002); [*Personal Information and Protection Act 2004* (Tas)](https://www.legislation.tas.gov.au/view/html/inforce/current/act-2004-046). [↑](#footnote-ref-29)
30. See *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13; *Human Rights Act 2004* (ACT) s 12; *Human Rights Act 2019* (Qld) ss 25, 66(1)(d), 73(4). [↑](#footnote-ref-30)
31. Government of South Australia, 2020. *Information Privacy Principles (IPPS) Instruction,* Premier and Cabinet Circular*,* PC012, May, cls 7-8. [↑](#footnote-ref-31)
32. Government of South Australia, 2020. *Information Privacy Principles (IPPS) Instruction,* Premier and Cabinet Circular*,* PC012, May. [↑](#footnote-ref-32)
33. Government of South Australia, 2020. *Information Privacy Principles (IPPS) Instruction,* Premier and Cabinet Circular*,* PC012, May, cl 6. [↑](#footnote-ref-33)
34. *South Australian Public Health Act 2011* (SA) ss 14(2), 14(5). [↑](#footnote-ref-34)
35. *Emergency Management Act 2004* (SA) s 31A. [↑](#footnote-ref-35)
36. Government of South Australia, 2020. *Information Privacy Principles (IPPS) Instruction,* Premier and Cabinet Circular*,* PC012, May, cl 4(1). [↑](#footnote-ref-36)
37. Ibid cl 4(2). [↑](#footnote-ref-37)
38. Ibid. [↑](#footnote-ref-38)
39. Ibid cl 4(2)(b)(c). [↑](#footnote-ref-39)
40. Ibid cl 4(3). [↑](#footnote-ref-40)
41. *South Australian* *Public Health Act 2011* (SA) s 49. A failure to comply with this request attracts a penalty of up to $25,000. [↑](#footnote-ref-41)
42. *South Australian Public Health Act 2011* (SA) s 4. [↑](#footnote-ref-42)