

4 December 2020

Our ref: KS:PV

Attorney-General's Department
4 National Circuit
BARTON ACT 2600

By email: [REDACTED]

Dear Review Team

Review of the Privacy Act 1988

Thank you for the opportunity to provide feedback on the issues paper for the review of the *Privacy Act 1988* (**the Issues paper**).

QLS is the peak professional body for the State's legal practitioners representing 13,000 Queensland registered legal practitioners. This response has been compiled with the assistance of the QLS Privacy and Data Law Committee whose members are practitioner volunteers with substantial expertise in privacy law.

QLS welcomes this review and thanks the Attorney General's Department (**the Department**) for the opportunity to make a submission. This submission highlights approaches and suggestions on key privacy law issues raised by the Issues Paper. Given the relatively brief time available for a response, this letter necessarily raises some high level issues only. This response does not purport to be a detailed submission on the extensive and important issues under review.

Objectives of the *Privacy Act 1988* (Cth) (Privacy Act**)**

QLS considers that a fundamental issue to be addressed is the jurisprudential bases of Australia's privacy laws is the treatment of personally identifiable information (**PII**). There are one or more overlapping possible legal areas involved; for example, consumer protection, human rights and property law, the latter involving notions of a fair exchange to individuals in return for commercial use of their PII and its derivatives.

A clear line of sight on these issues will inform and provide firm foundations for any reform decisions. Examples are decisions to be made on:

- Whether to adopt the human rights focus of the General Data Protection Regulation (**GDPR**) requirements for "legitimate bases" to exist for PII collections and disclosures, a matter having significant implications as regards privacy law's approach to biases in algorithmic decision making; and
- Whether it is appropriate for a consumer protection focus on awareness and informed consent to remain the cornerstone of Australia's legal approach to PII in the face of the practical difficulties in achieving this in an era of big data.

Review of the *Privacy Act 1988*

Definition of "Personal information"

There are some key concepts which those applying privacy laws do not find readily accessible from the Privacy Act's definition of PII. These are:

- the importance of perspective and context. In other words, that the same data might be PII to one collector but not to another because of the context and data matching capacity of the former versus the latter;
- the very important difference between anonymous and pseudonymous information; and
- the practical difficulties of understanding whether information is or is not PII for Privacy Act purposes because it is or is not "about" an individual.

QLS submits that there should be some legislative guidance to make the concept of PII more easily understood and accessible, by those who are not privacy lawyers.

Approach to Australian Privacy Principles (APPs)

QLS recommends against moving away from principles-based legislation to a more complex GDPR approach. Even a cursory view of the text of the GDPR will show that it defies meaning to those without legal or significant privacy professional experience. This is in contrast to the APPs. The text of the APPs has the benefits of adaptability to a range of circumstances and simplicity. QLS submits that if there is a desire for more detailed, prescriptive rules regarding privacy, the legislative response may be best suited by some delegated legislation on specific areas, for example the privacy rights of children and privacy in the context of algorithmic decision-making.

Exemptions

Small Business Exemptions

According to the ABS Counts of Australian Business, from at least 2017, 93% of Australian businesses had a turnover of less than \$2 million.¹ This means that currently nearly all business in Australia are not required to comply with the Privacy Act as 93% do not meet the \$3 million threshold. With only 7% of Australian businesses required to comply with the Privacy Act, QLS submits that the current exemption does not strike the right balance between protecting the privacy rights of individuals and the avoidance of unnecessary compliance costs.

Another concern which our members have raised with respect to the current small business exemption, is that it no longer reflects how businesses operate. For example, when the Privacy Act was amended in 2014, the digital economy was nowhere near as developed as it is now. With the increased use and reliance on eCommerce platforms such as *Shopify*, in many cases, small businesses are not holding personal information in isolation and have become intermediaries.

¹ ABS Counts of Australian Business 8165.0, Table 17, Feb 2019 and ASBFEO calculations (excludes nano businesses with no GST role), and ABS Counts of Australian Businesses, including Entries and Exits June 2015 to June 2019 8165.0, Turnover size, 20 Feb 2020.

Review of the *Privacy Act 1988*

Whilst it is likely that Shopify would need to comply with the Privacy Act, as it is the small business who is requiring individuals to provide personal information to a third party, we consider that a small business (or any business) should be required to undertake a due diligence process including a Privacy Impact Assessment before requiring individuals to provide their personal information to a third party. In this regard, we support the position of other submitters to the review that the Office of the Australian Information Commissioner (OAIC) should be resourced to assist small businesses to understand their obligations in this regard including to produce guidance materials.²

With over a million merchants and locations all over the world services such as Shopify,³ are targets for cyber attacks.⁴ The data risks associated with eCommerce platforms should require that all businesses, including small businesses, are required to comply with the Privacy Act in a manner which more fairly protects individuals from privacy risks. California with its CCPA legislation,⁵ in dealing with reasonable security, has adopted the CIS Controls, published by the Centre for Internet Security.⁶ QLS suggests that the OAIC might consider the CIS Controls in preparing its guidance notes for cybersecurity best practices.

Employee and Political Party Exemption

The current employee record exemption and the exemption for political parties is not sufficient to protect individuals.

With respect to employee records, QLS considers that the exemption should be removed, and all records should be captured under the Privacy Act. Firstly, removing the exemption would bring Australia in line with global best practice in connection with holding personal information.⁷ Unlike New Zealand, Australia is unable to be deemed as having adequate protections for the purposes of transacting with the EU, in part due to the exemptions provided for employee records. By obtaining adequate protection status, it will be easier for Australian businesses to compete on a global scale and deal with international organisations.

A second reason for the exemption to be removed is that increasingly, personal information about an employee falls into both categories. The exemption currently exempts the employer from complying with the Privacy Act when the personal information collected directly relates to a current employment relationship. This exemption becomes confusing when employers provide equipment such as mobile phones to their employees. For example, if the mobile phone has any type of tracking software or records when and where the phone is accessed, the information collected during working hours would be captured by the exemption. However, information collected outside of working hours would not be captured by the

² See submission of Salinger Consulting Pty Ltd, [Submission in response to the Privacy Act Review – Issues Paper, October 2020](#), at p 11.

³ "Empowering independent business owners everywhere", homepage, access Nov 2020, <https://www.shopify.com/>.

⁴ See for example: Notification made by PageUp People Limited to the OAIC on 12 June 2018, <https://www.pageuppeople.com/wp-content/uploads/2018/07/Eligible-data-breach-notification-to-OAIC-for-Web-Site.pdf>.

⁵ California Consumer Privacy Act of 2018.

⁶ [CIS Controls \(ciscsecurity.org\)](https://www.cisecurity.org/).

⁷ Witzleb, Normann, 31 July 2020, *he Conversation*, <https://theconversation.com/data-privacy-strict-european-rules-will-have-repercussions-in-australia-as-global-divisions-grow-142980>.

Review of the Privacy Act 1988

exemption resulting in the employer having to isolate the personal information and treat some of the information collected by the mobile phone as protected. This requirement to separate the information is unnecessary and confusing.

There are further reasons to remove the employee exemption to enable organisations to adopt one set of rules across their operations. Most organisations engage contractors as well as employees, and many of them manage PII of contractors and employees using similar processes and systems. Many organisations are structured as a group, with group entities that are not the employer, handling PII of another group entity's employees including through a shared services function. The recent decision in *Jeremy Lee v Superior Wood Pty Ltd*⁸ creates further potential inconsistency and confusion to operations, with the Privacy Act applying up to the point of collection of PII from employees, but the employee records exemption enlivened once collected.

The current exemption therefore in practice increases the risk of businesses breaching the Privacy Act unintentionally. If employers are having to treat some information as protected, it means that employers need to have processes in place to comply with the Privacy Act. If these processes are already in place to deal with isolated personal information, we submit that it would be easier to simply treat all information as protected.

Concerning personal information held by political parties, we submit that this exemption should be removed. There is no clear justification as to why political parties, who may hold comprehensive information about the public, should not be required to comply with the Privacy Act. Additionally, as political cyber attacks become more popular it is prudent that all levels of government have safe-guards in place.⁹ Similar to employee exemptions, removing this exemption will also bring Australia in line with global best practice in respect to the treatment of personal information.¹⁰

Notice of Collection of Personal Information

While serving some purposes, we recommend that the Department be cognisant of the limitations of collection notices.

We consider that in practice, collection notices often do not assist individuals in understanding and managing their PII. Notwithstanding OAIC guidelines, many entities provide lengthy collection notices and privacy policies to individuals partly driven to cover all the requirements under the Privacy Act. Many individuals do not read the collection notices including because of their length. Even where they are reviewed, we consider they often do not affect an individual's purchase or use of a good or service, where there is no or limited optionality provided to the individual concerning the proposed collection or handling of PII. We would advocate a collection notice regime with a greater emphasis on providing more limited information focussed on more obtrusive collection practices and uses. A short standardised framework would assist with this.

⁸ [2019] FWCFB 2946.

⁹ Crowe, David, 18 Feb 2019, Sydney Morning Herald, "Political parties should be stripped of Privacy Act exemptions after hack: experts", <https://www.smh.com.au/politics/federal/political-parties-should-be-stripped-of-privacy-act-exemptions-after-hack-experts-20190218-p50ymh.html>

¹⁰ Witzleb, Normann, above n 4

Review of the *Privacy Act 1988*

Consent

The review should consider whether opt in/consent requirements under privacy laws have, as a matter of technological progress, approached their use by date. Any informed choice concept needs to be workable for businesses and a practical reality for individuals. In an age of big data, machine learning and sensor-enabled consumer products, neither is often the case.

For example, if a person is deprived of employment opportunities because they do not engage with one of the leading job seeker platforms used by recruiters, then no amount of opt in or opt outs will provide a meaningful choice. This can readily be regarded as coercion and not voluntary consent.

We also observe that many businesses bundle consents in various clauses or paragraphs of their terms and conditions, privacy policies and collection notices. Obviously the OAIC's guidelines advocate against this practice, but it remains prevalent. Coupled with the fact that many individuals do not read such documents including when online by clicking to accept, we recommend that the Department considers with caution the control given to individuals by current consent mechanisms in the Privacy Act.

We also note that the limitations of the current consent model have been recognised by the UK Information Commission and the European Data Protection Board.¹¹ The UK's Information Commissioner's Office states that "Consent means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given and it will be invalid."¹²

The perceived easing of patent law restrictions following the 12 November 2020 decision of the High Court of Australia in *Calidad Pty Ltd & Ors v. Seiko Epson Corporation & Anor*,¹³ is likely to see an increase in data use and collection connected with consumer products because of the ease with which digitised consumer products involving patented components may be recirculated in trade following a first sale.

The consent approach adopted in the legislation could also better reflect that different degrees of safeguards are required depending on the specific uses that an organisation intends for collected data assets. An example can be seen in the protections adopted within the CCPA around the sale of personal information to third parties. Given the growing importance organisations place on big data insights and the growing prevalence of on selling, data sales should be closely examined within the context of consent.

A further issue with consent focused protections, is framing how long a given consent should remain valid, and where an organisation should be required to re-seek consent in the content of ongoing data collection, processing, sales or storing. This issue has practical privacy

¹¹ Presentation by Australian Information Commissioner and Privacy Commissioner Angelene Falk to the Law Council of Australia Media and Communications Seminar 2019: "Digital Platforms — The Future", 20 November 2019, < <https://www.oaic.gov.au/updates/speeches/privacy-implications-of-the-digital-platforms-inquiry/> >.

¹² UK Information Commissioner's Office, *What is valid consent?* < <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=Consent%20means%20giving%20people%20genuine,consent%20easily%20at%20any%20time.>> accessed November 2020.

¹³ [2020] HCA 41.

Review of the *Privacy Act 1988*

significant for individuals, given the extent of personal information over collection and the ad hoc approach many organisations adopt around data de-identification obligations.

The timeframes for which any consent given can be relied upon by the collecting organisation should also take into account the relevant circumstances, particularly where consent is often obtained from an individual within the context of the discreet provision of a specific, time-limited service or product. Many of the long term uses of collected data obtained within the context of this consent would not be within reasonable contemplation of the individual involved.

Timeframes upon which informed consents should remain valid is likely to receive increased global focus in the coming years, given regulators such as the UK Information Commission have acknowledged that under the GDPR “[c]onsent is likely to degrade over time [and that] how long it lasts will depend on the context.”¹⁴

QLS asks that the review consider the practical realities of applying any legal “consent” requirements.

Control and security of personal information

QLS submits that individuals should be in a position to expect a reasonable level of security to be in place in the protection of their personal information. The review should consider how the baseline cybersecurity standards which are being developed by Standards Australia,¹⁵ will interact with the Privacy Act.

There is a wide variety of approaches to privacy control and security requirements across Australian and international regulations. One example of legislation containing prescriptive security requirements for the protection of personal data is seen under the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. While the HIPAA is correctly credited with causing a measurable uplift in the privacy and security posture of the US healthcare and healthcare insurance industries, the approach created significant cost burden for many organisations and has occasionally been criticised for focusing attention on box-ticking activities as opposed to effective privacy risk management.

A prescriptive approach may also not be effective in the context of the Privacy Act given the broad range of organisations who are captured by the legislation and the need to avoid placing unnecessary compliance burdens on small businesses. If there are to be prescriptive requirements, we would suggest that these be tailored around recognised privacy investment and risk mitigation approaches such as the Australian Signal Directorates’ ‘Essential Eight’.¹⁶ Prescriptive provisions may also need to be subject to regular revision and update given the speed at which malicious actor methods change and the pace of privacy and security based innovations.

A potentially more effective approach, would be to adopt elements that are currently found within Australian Prudential Regulation Authority’s ‘*Prudential Standard CPS 234 Information Security (CPS 234)*’. A key element of CPS 234 is its underpinning risk assessment

¹⁴ UK Information Commissioners Office, What is valid consent? <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/>>

¹⁵ Braue, D, 25 Jun 2020, *Standards Australia to set cyber security standards*, available at <<https://ia.acs.org.au/article/2020/standards-australia-to-set-cyber-security-standards.html>>.

¹⁶ <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>.

Review of the *Privacy Act 1988*

obligations which require subject organisations to develop protection capability commensurate with their size and extent of the realistic threats posed to their key information systems and assets. This obligation creates a discipline for organisations by requiring them to gain situational awareness of both their key data assets and how realistic threats would arise in the context of their business. Situational awareness and an understanding of critical exposures are often overlooked traditional privacy risk management frameworks.

In the Australian context, the lack of effective situational awareness is common for many organisations, particularly where a strong outsourced model is used that relies on externally managed services providers to deliver privacy and information security solutions. There is regular dissidence between what these vendors promise, and the practical reality of the services that an organisation receives, which is only identified after a significant privacy compromise or data security event has occurred.

A genuine uplift in privacy compliance behaviour in Australia is likely to be achieved where elements of the outsourcing privacy compliance model can be challenged, for example by imposing common sense risk assessment and situational awareness obligations that sits within the organisation itself.

While third parties could be relied on to assist with this risk assessment process, we would recommend including a requirement that any third party risk assessment provider be independent and not part of an ultimate service provider retained to deliver privacy, availability and information security services. This would also help address key concerns seen within supply chain cyber risk exposures. We accept that small and medium enterprise organisations may need to be exempt from obligations of this nature, to avoid unnecessary compliance costs.

Access to, and correction of personal information

Consideration should be given to amendments which allow individuals to have greater access to and the ability to correct, personal information which is collected and used. We have had the benefit of reviewing the submission by Dr Kate Mathews Hunt to the review and we share similar concerns about the inability to access and indeed challenge algorithmic biases.

We agree that, where possible, an individual's personal information should be accessible and that the review should consider a right to erasure in appropriate circumstances.

Overseas data flows and third-party certification (Transborder data flows)

QLS submits that the strict liability to which Australian business PII transferors are subject under s 16C of the Privacy Act and APP 8 is too stringent for Australian business transferors. Part of the review should be to assess how this strict liability regime has influenced the practice of privacy law, if at all, and the extent to which there have been any known interferences with privacy based on this regime.

QLS suggests that a better approach would be to assist Australian businesses to comply by promulgating model contract clauses, similar to those available for US-EU-UK transfers, and incentivising compliance by triggering sanctions when and if there is a failure to monitor and take remedial steps regarding non-compliance.

Direct right of action

A direct right of action must be framed such that the process of seeking compensation is both simple and inexpensive for individuals impacted by an interference with privacy. Otherwise,

Review of the *Privacy Act 1988*

there is a risk the direct right of action will provide limited recourse for individuals beyond the existing dispute resolution mechanisms in the *Privacy Act*.

In the Digital Platforms Inquiry (DPI) final report,¹⁷ the ACCC recommended that consumers be given a direct right of action both in their individual capacities and by way of class action. The inclusion of the class action recommendation, in respect of interferences with privacy impacting multiple individuals, was important to facilitate the efficient and cost-effective access to compensation for individuals. However, since the DPI report was released, concerns about litigation funding and the regulation of the class action industry have culminated in the Parliamentary Joint Committee on Corporations and Financial Services (PJCCF) holding an inquiry into these issues.¹⁸ The PJCCF will issue its final report, which is expected to address issues such as the inclusion of contingency fees in Federal Court class actions and the broader economic impacts of the class action regime, in December 2020. Until the release of the PJCCF's final report, it is unclear whether class actions will be an appropriate solution for individuals seeking to cost-effectively pursue direct rights of action.

Another potential solution discussed in the Issues Paper is to allow individuals the option of seeking conciliation with the (OAIC (or some other administrative body) or applying directly to the courts, consistent with the application of the Consumer Data Right (CDR) enacted under the *Competition and Consumer Act 2010* (Cth) (CCA).¹⁹ Providing impacted individuals with complementary regulatory and private actions allows them to pursue complaints which the OAIC does not consider worth pursuing, and vice-versa.

However, absent allowances for class actions or other means for limiting costs, an impacted individual who elects to pursue litigation is still faced with significant costs and inconvenience. It should also be noted that the direct right in favour of CDR consumers may be pursued by way of class action.

Statutory tort

QLS agrees that a statutory tort for invasion of privacy is needed.

The creation of a statutory tort for invasion of privacy has been recommended by a number of significant National and State inquiries. These include, but are not limited to:

- The Australian Law Reform Commission's 2008 report, 'For Your Information: Privacy Law and Practice' which recommended that Commonwealth legislation should provide for a statutory cause of action for serious invasion of privacy;²⁰
- The 2016 Standing Committee on Law and Justice, Parliament of New South Wales, 'Remedies for the Serious Invasion of Privacy in New South Wales' report which recommended that the NSW Government introduce a statutory cause of action for serious invasions of privacy;²¹

¹⁷ <https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf>

¹⁸ https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Corporations_and_Financial_Services/Litigationfunding

¹⁹ <https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf>.

²⁰ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice, Report 108* (2008) Rec 74-1, at p 88.

²¹ Standing Committee on Law and Justice, Parliament of New South Wales, *Remedies for the Serious Invasion of Privacy in New South Wales* (Report, March 2016) at p 10.

Review of the *Privacy Act 1988*

- The 2016 South Australian Law Reform Institute, 'A statutory tort for invasion of privacy' report;²² and
- The ACCC's 2019 DPI Final Report (**the Digital Platforms Inquiry**) which recommended the introduction of a statutory tort for serious invasions of privacy.²³

In 2014 the Australian Law Reform Commission (**ALRC**) was asked to design a cause of action in its 'Serious Invasions of Privacy in the Digital Era (ALRC Report 123)' report noting that three recent law reform inquiries had already affirmed that a cause of action was desirable.²⁴

In a submission to the Digital Platforms Inquiry, the United Nations Special Rapporteur on the right to privacy said:

*It is clear that within Australia, there has been considerable work done by eminent inquiry bodies at the Federal and State levels, that has seen each inquiry support the enactment of a statutory cause of action for serious invasions of privacy. These inquiries also have included comprehensive consultation with key stakeholders. Despite these recommendations and the consultations, no Federal or State government has introduced such legislation...*²⁵

QLS agrees with the various legal and other stakeholders that a statutory tort is appropriate and long overdue.

Support for legislative reform has also been highlighted by statutory and regulatory bodies. For example, in its 'Operation Impala; Report on misuse of confidential information in the Queensland public sector' in February of this year,²⁶ the Crime and Corruption Queensland (**CCC**) recommended that the Queensland Government 'consider the introduction of a statutory tort for serious invasion of privacy by the misuse of private information, such as by collecting or disclosing private information about the plaintiff'.²⁷ The CCC's recommendation relates to the misuse of private information in the public sector but its report highlighted that 'Australia is behind many other countries where statutory torts for privacy exist'²⁸ and reflects a long standing call for legislative progress on these issues.

²² South Australian Law Reform Institute, [A statutory tort for invasion of privacy](#) (Final Report, March 2016) at p 26.

²³ Australian Competition and Consumer Commission, [Digital Platforms Inquiry Final Report](#), June 2019 at p 493.

²⁴ Australian Law Reform Commission, 14 July 2014, *Should a new tort be enacted?*, available at <<https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/1-executive-summary/should-a-new-tort-be-enacted/>>.

²⁵ UN Special Rapporteur on the Right to Privacy, [Submission to the ACCC Digital Platforms Inquiry](#), February 2019, at p 8.

²⁶ Crime and Corruption Commission Queensland, [Operation Impala; Report on misuse of confidential information in the Queensland public sector](#), February 2020, Rec 17.

²⁷ Crime and Corruption Commission Queensland, [Operation Impala; Report on misuse of confidential information in the Queensland public sector](#), February 2020 at p 19.

²⁸ Crime and Corruption Commission Queensland, [Operation Impala; Report on misuse of confidential information in the Queensland public sector](#), February 2020 at p 128.

Review of the *Privacy Act 1988*

The ALRC have previously outlined the benefits of statutory reform in this area and we agree that a statutory tort is preferable.²⁹ QLS considers that the legislature is best able to respond with the requisite flexibility to adapt to evolving technologies and to ensure that the cause of action is appropriately targeted and includes options for alternative dispute resolution.

Notifiable data breach scheme

QLS welcomes the general approach of the Privacy Act's notifiable data breach scheme. In general terms, we are of the view that this fosters compliance. It does this by incentivising early assessment and notification as a precursor to any follow on privacy interference finding.

The drafting of the notifiable data breach scheme also has the advantage of offering data holders a clear decision flow, assisted greatly by practical documents such as the flowchart published by the OAIC.

Despite general support for the scheme, QLS considers that the following matters require further consideration as part of the review:

- uncertainty as regards the "risk of harm" test;
- uncertainty as to the entities/ies who have primary notification responsibilities under the scheme. They are "holders" of the PII. Because the Privacy Act does not reference notions of "controllers" and processors" like GDPR, there is significant scope for confusion as to roles and responsibilities under the scheme. This is particularly important when any one data platform suffering a data breach scenario has many application programming interfaces (API) to other platforms and a great many contracted support providers;
- the need for greater legislative guidance about how the scheme interacts with domestic and international laws, for example where a data breach scenario impacts on individuals in many countries.

Interaction between the Privacy Act and other regulatory regimes

Symptomatic of the increasing ubiquity of data law issues impacting on the public and privacy sectors, there has been an exponential increase in the number of Australian Commonwealth and State legislative data law initiatives and reviews in recent times. By way of example, over the past 12 months QLS's Privacy and Data Law Committee has considered the following, to name a few:

- data law issues with respect to government access to vehicle-generated data;
- privacy and information security issues relating to the Queensland government's proposed digital licence app and camera enforcement of seatbelt and mobile phone offences; and
- the interaction between human rights, technology and artificial intelligence

On a day-to-day basis, legal and business advisers need workable tools to navigate this increasingly complex and important field. QLS asks that the review address this. For example, consideration might be given to how to enhance cohesiveness and alignment across agencies and lawmakers with respect to data treatment. One consideration might be a master

²⁹ Australian Law Reform Commission, 14 July 2014, *Should a new tort be enacted?*, available at <<https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/1-executive-summary/should-a-new-tort-be-enacted/>>.

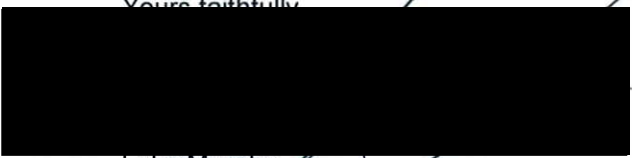
Review of the *Privacy Act 1988*

set of privacy and data law principles, capable of legislative cross-referencing and adaptation on a case by case basis.

QLS would welcome the opportunity to discuss these concerns with you further and to participate in any workshops or sessions which the Department might host concerning the review. We look forward to providing further submissions to the review in due course.

If you have any queries regarding the contents of this letter, please do not hesitate to contact our Legal Policy team via policy@qls.com.au or by phone on (07) 3842 5930.

Yours faithfully,



Luke Murphy
President