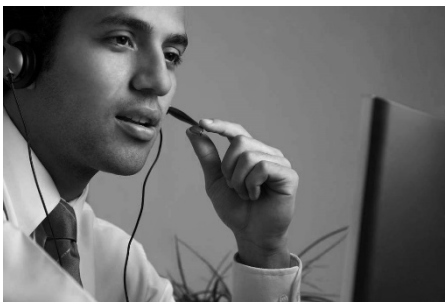
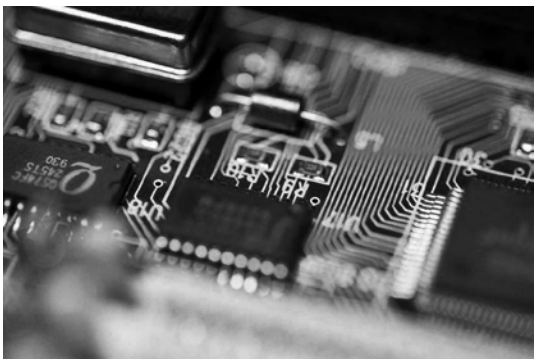
Data-sharing and privacy

Submission to the Productivity Commission's *Inquiry into Data Availability and Use*

29 November 2016





SalingerPrivacy

We know privacy inside out.

Covering letter

29 November 2016

Mr Peter Harris AO
Chairman
Productivity Commission
Level 12, 530 Collins Street
Melbourne VIC 3000

Dear Mr Harris,

This submission addresses the following draft recommendations of the *Data Availability and Use : Draft Report*, 3 November 2016:

- Recommendation 5.1 (OAIC to create de-identification guidelines and certify practices)
- Recommendation 5.2 (fix the research exemption)
- Recommendation 5.4 (data custodians' responsibilities)
- Recommendation 9.1 (definition & regulation of "customer data"), and
- Recommendation 9.2 (proposed new privacy rights).

I have no objection to the publication of this submission.

Please do not hesitate to contact me if you would like clarification of any of these comments.

Anna Johnston
Director | Salinger Privacy

Introduction

In making this submission on behalf of Salinger Privacy, I do not represent or claim to speak on behalf of any of our clients. My views are informed by my experience from over 15 years working exclusively in the privacy law field, as a specialist privacy consultant and before that as a regulator. My qualifications are set out at the end of this submission.

It is my submission that if you want to increase the use of data-sharing for the public good, you need two conditions:

- First, you need data custodians to feel they are on solid legal ground when they decide to release data; and
- Second, you need public trust.

This submission addresses these two elements, by commenting on the following draft recommendations from the *Data Availability and Use : Draft Report*, 3 November 2016:[1]

- Recommendation 5.1 (OAIC to create de-identification guidelines and certify practices)
- Recommendation 5.2 (fix the research exemption)
- Recommendation 5.4 (data custodians' responsibilities)
- Recommendation 9.1 (definition & regulation of "customer data"), and
- Recommendation 9.2 (proposed new privacy rights).

[1] http://www.pc.gov.au/inquiries/current/data-access/draft

Assistance for Data Custodians

Recommendation 5.1 (OAIC to create de-identification guidelines and certify practices)

I agree that more detailed guidance is needed on the topic of de-identification, and the level of debate about this topic at the Information Commissioner's recent workshop[2] suggests that in fact these guidelines could potentially be in the form of a standard.

However I express some reservations about the idea of the Office of the Australian Information Commissioner (OAIC) then having a role in *certifying compliance* with that standard.

Not only does that likely pose a resourcing difficulty for the OAIC, but in my view would also pose a conflict of interest, because the OAIC is the regulator in the event of a privacy complaint about either a breach of the standards, or a privacy breach that occurred despite compliance with the standard - which might then suggest that the standard was not keeping up with developing re-identification techniques, for example.

I would suggest that this role might be more appropriate for the proposed new National Data Custodian, although with a requirement that the guidelines or standards must be subject to consultation with, or the agreement of, the Privacy Commissioner. That would be a similar model to the National Health and Medical Research Council (NHMRC) guidelines on research involving personal information.[3]

In terms of the content of the guidelines or standard, I suggest a layered or contextual approach will be needed. For example, one standard would be: "what is the degree of de-identification needed to render something no longer 'personal information', such that the privacy principles don't apply at all?"

That is a different question to: "what is the degree of de-identification needed to allow for the use or disclosure of this data under a research exemption?" And even within that question, there are layers.

You might for example allow a lower standard of de-identification if there are other privacy controls in place, such as the use of data enclaves, and/or if the nature of the personal information at issue poses a low risk to the subjects if it were to be re-identified. Higher standards would be required for open release of data. The de-identification guidelines or

[2] See the debate on Twitter at https://twitter.com/hashtag/deidworkshop?src=hash and the panellists at http://www.govinnovate.com.au/program/session/day-3--wednesday-16-november-2016_workshop-a-data-sharing-and-interoperability-panel-of-experts-covering-legal-privacy-and-technical-aspects-sold-out/

[3] See http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s95.html

standards will therefore need to be nuanced. Ideally they would also grapple with questions such as "how do we de-identify personal information that is in x-rays or tissue samples?"

Recommendation 5.2 (fix the research exemption)

I agree that the research exemption in the *Privacy Act 1988* (Cth) needs fixing. When the Act was reformed in 2014 and the privacy principles streamlined into one set instead of two, the research exemptions were sadly not also unified. We therefore still have one exemption for the public sector, and one for the private sector, saying different things, and both artificially restrictive.

Section 95 regulates the public sector. It covers *any* personal information, and exempts *all* Australian Privacy Principles (APPs), but only in relation to 'medical research' – a term which is undefined other than to include epidemiological research. By contrast section 16B, which regulates the private sector, covers only *health* information, and only the collection, use and disclosure APPs, for research 'relevant to public health or public safety' – also undefined. Each is subject to separate guidelines developed jointly by the NHMRC and Privacy Commissioner.

A better formulation, which would also more closely align with State privacy laws, would be to allow for all regulated entities an exemption from the APPs relating to collection, use or disclosure of any type of personal information, "for the purpose of research in the public interest", but subject to guidelines developed jointly by the NHMRC and Privacy Commissioner. The need for ethical review, rules about de-identification, and the circumstances in which it may be appropriate to proceed in the absence of the subject's consent, should also be built into the test, as now.

Recommendation 5.4 (data custodians' responsibilities)

In my view this recommendation does not really address the problem of the under-resourcing of data custodians to process data requests. It just adds extra reporting requirements on them. Instead, I believe that data custodians need more pragmatic assistance to understand and apply the law governing their use and disclosure of data.

My view is that the ideal law sets *tough* standards that are nonetheless *easy* to comply with.

My experience over many years working with government clients is that the wording or 'toughness' of the rules themselves is almost irrelevant to the individual who needs to apply them. What matters to that decision-maker is how quickly and easily the standards can be found, understood, and followed.

For example, put yourself in the shoes of Phil the physiotherapist, or Sue the Centrelink manager, or Shari who is rostered on the front counter at a business. An insurance company investigating a personal injury claim has asked to see their file on Joe Bloggs. Phil and Sue

and Shari don't know whether they're allowed to hand it over. Their primary question is: "Can I disclose this information?"

And likewise, the custodian of datasets of public value wants to know: "Can I lawfully disclose *this* information, in *this* format, in *these* circumstances, to *this* person or body requesting it?"

To answer any one of these questions can often involve a painstaking task of navigating through privacy principles, and exemptions, and applying the case law. It's a lot easier to just say "no", and blame "privacy".

Instead, I would like to see the process of navigation made much simpler.

Earlier this year we developed a tool for organisations regulated under NSW privacy laws, which includes not only State and local government agencies, but also private sector organisations operating in NSW that hold 'health information'. We mapped out the NSW Disclosure rules under the two NSW privacy statutes into a flowchart based, question-and-answer format, to guide decision-making. Because of all the different exemptions and special rules for different types of personal information, the flowcharts run over seven pages – but the user can move through them quickly.[4]

Our new *Untangling Privacy* flowcharts guide works together with our annotated guide to the NSW privacy laws, *PPIPA in Practice*, which explains the interpretation on offer from both the Privacy Commissioner and case law about what each part of each test of each rule means in practice. There is a very high volume of privacy case law generated in NSW, so we update our guide every quarter.[5]

But our guides are effectively still in analogue form. We would love to have the time and funding to turn our two guides into a properly automated and digital tool: an app so that users can very quickly get to the correct rule for their situation, and can also click through to see up-to-date interpretation of that rule.

In an ideal world, the app would also be made available to the public for free. In our view this would also help consumers exercise control over their data, if they could more easily understand what the privacy laws actually allow for.

It is therefore my submission that if the objective is to break down barriers to data-sharing for the greater public good, the government should fund the development of this type of guidance to applying privacy law, by way of an online, automated tool, to allow all types of data custodians, both big and small, to really quickly figure out their answer, each time they are approached with a request to share or disclose the data that they hold. There would be no more hiding behind "because of the Privacy Act".

---

[4] *Untangling Privacy*, available at http://www.salingerprivacy.com.au/downloads/untangling-privacy-disclosure-ebook/
[5] *PPIPA in Practice*, available at http://www.salingerprivacy.com.au/downloads/ppipa-in-practice/#1

Protections for consumers

The second half of the equation needed to facilitate greater data-sharing is to engender public trust. I suggest that to gain the kind of public or consumer trust necessary to allow for more data-sharing, you have to make every effort to ensure:

(i) That every possible step is taken to prevent things going wrong, but also…

(ii) That people will be protected in the event that something *does* go wrong.

Prevention of data breaches requires better education of both data custodians and policy-makers. I note that Alastair MacGibbon, in his recent review of the Census, has recommended the idea of a 'Cyber Bootcamp' for Ministers and senior public servants.[6] I think that is a brilliant idea, and I suggest that there should be a 'Privacy Bootcamp' as well.

But while prevention is better than the cure, we need to ensure there are cures as well. Our system of statutory privacy principles is not enough. There are many privacy breaches which cause individuals harm, for which they currently cannot seek a remedy.[7]

If you want to promote greater data-sharing, you will need to convince the public that their privacy is going to be protected – or that if all else fails, they will be compensated for any significant harm that they suffer. In my view, that means that the Government should take greater steps to offer remedies for people who suffer serious privacy harm, in parallel with any steps to increase the level of risk posed to individuals from greater data-sharing.

The Government currently has two privacy-related Bills before Parliament, one of which is the data breach notification bill,[8] and the other is a proposal to criminalise the re-identification of 'de-identified' government datasets.[9] However neither of those Bills will actually provide remedies for victims of privacy invasions.

I suggest that if the Government is serious about this issue, it should not proceed with legislation to increase the amount of data-sharing without *first* legislating to create a statutory tort of privacy, as recommended by the Australian Law Reform Commission,[10] and other inquiries.[11]

---

[6] See https://t.co/He3E84CqiL
[7] For various examples of privacy breach victims unable to obtain remedies, see our blog on this topic at http://www.salingerprivacy.com.au/2015/08/25/the-privacy-law-reform-merry-go-round/
[8] See http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5747
[9] See http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1047
[10] See http://www.alrc.gov.au/inquiries/invasions-privacy
[11] See https://www.parliament.nsw.gov.au/committees/inquiries/Pages/inquiry-details.aspx?pk=1877#tab-reports

Recommendation 9.1 (definition & regulation of "customer data")

I disagree with this recommendation. I suggest that a new definition of "customer data" would lead to regulatory duplication and confusion. The types of data proposed to be regulated already fit, in my view, within the definition of 'personal information' in the *Privacy Act 1988* (Cth).

If the definition of 'personal information' is seen as in need of clarification, this can be done in other ways, such as by OAIC guidelines or a 'Note' added to the Privacy Act, for example to state that personal information includes inferences generated from other data. The definition may need clarification anyway, depending on the outcome of the Grubb v Telstra case.[12]

Recommendation 9.2 (new privacy rights)

Likewise, I would suggest that there is no need to create a new legal regime offering specific rights for "customer data". APPs 12 and 13 already offer access and correction rights.

I would suggest that instead, APPs 12 and 13 could be strengthened, by allowing for the individual to specify in their access request if they want the personal information in machine-readable format.

The right to 'appeal automated decisions' could be dealt with by strengthening APP 10, the Data Quality principle, and/or by specifying that a remedy for a breach of APP 10 is the right to appeal, or have reviewed, a decision made in reliance on their personal information.

With respect to the proposed right to 'opt out' of data collections, I express some reservations about how this might work in practice, given the large number of exemptions that would be needed, as already identified in your draft report. The APPs already require that entities limit their collection of personal information to that which is reasonably necessary or directly related to a function or activity of the entity; and in relation to 'sensitive information' they may also need the subject's consent.

I would be concerned that by offering an 'opt out' option, rather than delivering on the intended objective of *improving* consumers' control over their data, it might undermine the existing Collection Limitation principle and exacerbate the problem of over-collection. Businesses might take a more expansive view of 'let's collect everything we can until we are told not to', on the basis that only a few will ever read the fine print and ask them to stop.

If the objective is to improve consumers' control over the collection of their data, I suggest that resources should instead be dedicated to better understanding and enforcement of the existing Collection Limitation and Data Retention principles, as well as APP 13 in relation to the right to seek the deletion of data no longer needed.

---

[12] For an explanation of the implications of that case, see our blog at http://www.salingerprivacy.com.au/2016/02/23/how-stephanies-broken-down-car-is-undermining-your-privacy/

Qualifications

The comments in this submission do not constitute legal advice, and should not be construed or relied upon as legal advice by any party. Legal professional privilege does not apply to this submission.

About the author

This submission has been prepared by Anna Johnston, Director, Salinger Privacy.

Ms Johnston was previously the Deputy Privacy Commissioner of NSW. She holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. Anna was admitted as a Solicitor of the Supreme Court of NSW in 1996, and is an accredited mediator.

Ms Johnston is a past Chair of the Australian Privacy Foundation, was a founding member and Board Member of the International Association of Privacy Professionals, Australia & New Zealand, and for many years sat on the editorial board of the Privacy Law Bulletin. She served on the Australian Law Reform Commission's expert advisory group on health privacy, and was primary author of the Australian chapter for Privacy International's *Privacy & Human Rights*. She was also called upon to provide comment to the European Commission on the adequacy of Australia's privacy laws.

Salinger Privacy offers specialist privacy consulting services, training and publications. Our consulting services include Privacy Impact Assessments and privacy audits. Our training programs include both face-to-face and online privacy awareness training programs, as well as specialist workshops on Research & Privacy, privacy risk management and Privacy by Design. Our publications include Big Data – An Ethical Framework for Protecting Privacy, a quarterly subscription-based annotated guide to NSW privacy law, and a monthly blog and newsletter.

We know privacy inside out.

Salinger Consulting Pty Ltd
ABN 84 110 386 537
PO Box 1250, Manly NSW 1655
www.salingerprivacy.com.au