Does data sharing complement or challenge privacy law?

David Kreltszheim CORNWALL STODART

The expected benefits of "big data" for citizens, government and business alike have led to a strong policy push for a new data sharing law. The new law will complement the Privacy Act 1988 (Cth) by giving individuals and small businesses a new comprehensive access right to digital "consumer data". On the other hand, the new law proposes a sweeping open public sector digital data access regime. Assessing the risk that ostensibly de-identified data may be re-identified is central to the privacy impact of the new law and creates significant challenges for confidentiality and privacy.

Comprehensive right of access

The Productivity Commission (the Commission) has recommended that a "consumer" be given a new comprehensive right to access digital consumer data held by a data holder (Comprehensive Right).[1]

A consumer will include single persons, family groups or other groups resident at a single address in the data holder's dataset, and any entity with an Australian Business Number (ABN) and a turnover of $3 million per annum or less.[2]

Consumer data is to have an outcome-based definition, broadly covering data that is sufficient to enable the provision of a competing or complementary service or product for a consumer. The scope of the definition for a particular industry will be set out in a data specification agreement for that industry, to be registered with the Australian Competition and Consumer Commission.[3] Data that is unable to be re-identified to a consumer in the normal course of business within a data holder will not be considered consumer data.

The Comprehensive Right will enable consumers to:[4]

- have access to, and use, their consumer data jointly with the data holder, in perpetuity
- direct data holders to transfer data in machine-readable form, either to the consumer or to a nominated third party
- request edits or corrections to their consumer data for reasons of accuracy
- be informed of the trade or other disclosure of consumer data to third parties

Broadly, the Comprehensive Right would enhance consumers' ability to have their consumer data used for the provision of a service that competes with, or complements, the service that the data holder provides to the consumer. For example, by enforcing the Comprehensive Right, a consumer might be able to improve their personal finance decisions, compare complex service offerings, obtain personalised products and services, and prompt more competitive pricing from competing product or service providers.[5] This would be good news for emerging tech (and especially fintech) companies with business models based on gaining access to consumer data held by an incumbent service provider like a bank.

The Australian Privacy Principles in the Privacy Act will continue to apply to a data holder in its handling of consumer data that is personal information.[6] But the Commission has recommended additional protections for the handling of consumer data, as follows:[7]

- All holders of consumer data should include in their privacy policies, terms and conditions; or on their websites, a list of parties to whom consumer data has been traded or otherwise disclosed in the past 12 months.
- On the wind-up of an entity that holds consumer data, consumers should be informed if data for which they hold a joint right has been traded or transferred to another entity (if the transferring entity is subject to a formal insolvency process, the insolvency practitioner must ensure that consumers have been informed of these trades or transfers).

As any entity with an ABN and a turnover of $3 million per annum or less will be treated as a consumer for the purposes of the Comprehensive Right, the protections for consumer data will extend to data relating to small businesses, not just to individuals' personal information.

In summary, the Comprehensive Right will complement the Privacy Act by:

- giving small business entities rights in relation to their consumer data where they had none under the Privacy Act

- giving individuals the benefit of additional protections which, although analogous to protections under the Privacy Act, have a different content and are imposed for a different purpose

Public sector open data access

In parallel with the creation of the Comprehensive Right, the Commission has recommended a new data sharing and release structure that would promote more open access and use of digitally held public sector data, publicly funded research data, and data held by entities regulated or funded for public purposes (Public Sector Open Access).[8]

Public Sector Open Access would facilitate greater access to, and use of, data held by the public sector and by entities regulated or funded for public purposes. To the fullest extent constitutionally possible, Public Sector Open Access is intended to permit state government data holders to become integrated with Commonwealth government data holders for the purposes of the sharing and linkage of data.[9] Data holders would continue to be subject to applicable privacy laws to the extent that the digital data they handle is personal information.

"Doing nothing is not an option"

Why has data sharing became an issue? The Commission notes that advances in data analytics will create significant opportunities for groundbreaking new products and services, and improved government and business processes.[10] The examples that it gives include:

- better healthcare outcomes for individuals through improved identification of population heath issues, and improved patient management and resource allocation using triage algorithms[11]
- online businesses (for example Google and Facebook) generating commercial value by applying novel analytic techniques to rich datasets and logistics businesses (for example, United Parcel Service (UPS)), increasing efficiency through real-time route optimisation, crowd-based pick-up and delivery, strategic network planning and capacity planning[12]

In this light, the Commission considers that fundamental changes need to be made to the legal and policy frameworks in which public and private data are handled in Australia.[13] The Commission's view is that:

- we have been "nervous about making decisions"[14] and "uncertainty [has] endorse[d] inaction"[15]
- as the nature of data sources and data analytical techniques are evolving rapidly and will continue to do so, "doing nothing is no longer an option"[16]
- while the protections that apply to personal information under the Privacy Act will remain in place, data availability should not just be viewed through a privacy lens[17]

Administering the new law

The Commission has recommended that a new Commonwealth Data Sharing and Release Act should establish the Comprehensive Right[18] and create a National Data Custodian to administer Public Sector Open Access.[19] The Commission has explicitly cautioned against the government decoupling parts of the reform framework that it has recommended.[20] How might that decoupling occur?

First, the government may at least initially seek to apply the principles of data openness and sharing to digital data in limited areas only. The quality and consistency of a range of datasets, data definitions and formats could be improved, and significant benefits generated, from the wider sharing and release of several types of data with minimal or no privacy or confidentiality risks. Examples include data on hydrology, flora and fauna, mineral and energy resources, fisheries, forestry, and agriculture to name just a few areas. I think this is unlikely given the benefits that would undoubtedly flow from having a data sharing and release mechanism that covers all digital data, even where the handling of that data involves some degree of risk of the compromise of individuals' privacy and individuals' and businesses' confidentiality.

Second, the government may seek to implement different rules for the handling of "low risk" digital data of the kind described above as compared to digital data the handling of which involves a degree of privacy and confidentiality risk.[21] At some level, I think that this is inevitable. The Commission itself acknowledges that approaches to reducing the identifiability and sensitivity of data are of interest to its inquiry given the focus of the inquiry on enabling digital data to be made more widely available.[22] The "bright line" for when privacy and confidentiality will be adequately protected when digital data is shared or released is whether the data in question is "de-identified". This means that data identifying an individual or business has certain variables removed or encrypted to suppress the identification of the individual or small business from that data.[23]

Third, could the government be tempted to split the regulation of the data sharing and release regime so that the Office of the Australian Information Commissioner (OAIC) is responsible for the regime in so far as it concerns digital data the handling of which may affect individuals' privacy (and perhaps even businesses' confidentiality)? The Commission's view is that this would not be appropriate.[24] The government has created a

cross-portfolio task force in response to the inquiry, recognising the multifaceted nature of the reforms needed for data availability and use.[25] I suggest that there is a significant role to be played by the OAIC in the crucial area of the de-identification of digital data and the assessment and treatment of re-identification risks.

Assessing and treating re-identification risks

From the above, it is evident that the assessment and treatment of re-identification risks are central to the privacy impact of the new law. In recent years, OAIC has issued guidance on de-identification of personal information by businesses[26] and agencies.[27] Additionally, the OAIC and the Commonwealth Scientific and Industrial Research Organisation's (CSIRO) Data61 have released a guide that is an important starting point for a more nuanced, practical and risk-based understanding of how organisations and agencies should make decisions about the de-identification of data.[28] Agencies and organisations which are not familiar with the technical and risk management aspects of assessing re-identification risks will have to acquire new skills in the coming months and years.

David Kreltszheim
Special Counsel
Cornwall Stodart
D.Kreltszheim@cornwalls.com.au
www.cornwalls.com.au

The views expressed are the author's own and do not necessarily reflect those of Cornwall Stodart.

Footnotes

1. Productivity Commission (Cth) *Data Availability and Use — Inquiry Report* Report No 82 (2017) 199 (recommendation 5.1).
2. Above n 1, at 198.
3. Above n 1, at 210 (recommendation 5.2).
4. Above n 1, at 199 (recommendation 5.1).
5. Above n 1, at 100–4.
6. Above n 1, at 202, 310 and 336.
7. Above n 1, at 214 (recommendation 5.3).
8. Above n 1, at 239–43 (recommendations 6.1, 6.2, 6.3 and 6.4).
9. Above n 1, at 311–12.
10. Above n 1, at 4–8, 57–64 and 99–119.
11. Above n 1, at 104.
12. Above n 1, at 107.
13. Above n 1, at 12.
14. Above n 1, at 12.
15. Above n 1, at 12.
16. Above n 1, at 12.
17. Above n 1, at 14.
18. Above n 1, at 312 (recommendation 8.1).
19. Above n 1, at 249 (recommendation 6.6).
20. Above n 1, at 30.
21. Cf the submission to the Commission recommending that the inquiry into data availability and use be split into two segments — one addressing personal data specifically, the other addressing other categories of data: Xamax Consultancy, Submission No 3 to Productivity Commission, *Data Availability and Use — Inquiry Report* (5 May 2016) 2.
22. Above n 1, at 56 and 96–8.
23. Above n 1, at 56.
24. Above n 1, at 310.
25. Department of the Prime Minister and Cabinet (Cth) "Data Availability and Use Taskforce" (9 May 2017) www.pmc.gov.au/public-data/data-availability-and-use-taskforce.
26. OAIC "Privacy business resource 4: de-identification of data and information" (April 2014) www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-4-de-identification-of-data-and-information. For commentary, see S Klimt, D Kreltszheim and T Lirosi "When bright lines blur: when is personal information 'de-identified' and why does it matter?" (12 May 2016) www.claytonutz.com/knowledge/2016/may/when-bright-lines-blur-when-is-personal-information-de-identified-and-why-does-it-matter.
27. OAIC "Information policy agency resource 1: de-identification of data and information" (April 2014) www.oaic.gov.au/information-policy/information-policy-resources.
28. CM O'Keefe, S Otorepec, M Elliot, E Mackey and K O'Hara *The De-identification Decision-Making Framework* CSIRO Report Nos EP 173122 and EP 175702 (2017).