Office of the Information Commissioner
Queensland

Submission to the Australian Government Productivity Commission

Data Availability and Use

July 2016

Introduction

The Queensland Office of the Information Commissioner is an independent statutory authority. This submission does not represent the views or opinions of the Queensland Government

The Office of the Information Commissioner's (OIC) statutory functions under the *Right to Information Act 2009* (**RTI Act**) and *the Information Privacy Act 2009* (**IP Act**) include assisting in achieving the goal of open and transparent government by promoting better and easier access to public sector information and improving the flow of information to the community balanced with appropriate protections for certain information, including personal information. Through its functions, OIC supports the public sector's corporate governance and accountability framework.

There is increasing recognition in democratic countries across the world of the benefits of openness, transparency and accountability. Greater openness and transparency delivers a range of tangible benefits including greater public engagement, improved service delivery and restoring trust and confidence in government.[1] As noted by the OECD, trust in institutions including government continues to decline and only 40% of citizens trust their government.[2]

Queensland's RTI Act recognises that government-held information is a public resource and that openness in government enhances accountability. The RTI Act represents a clear move from a 'pull' model' to a 'push model' emphasising proactive and routine release of information and maximum disclosure of information unless to do so would be contrary to the public interest. The RTI Act states that a formal application for government-held information under the RTI or IP Act should only be made as a last resort. Federal, State and Territory governments have their own Freedom of Information or RTI legislation.

At a national level, the Australian Government has committed to finalising membership of the Open Government Partnership (OGP) and public consultation was undertaken to develop an Australian Government National Action Plan for open government. The OGP is a voluntary, multi-stakeholder international initiative created to promote transparency,

In principle, information held by government should be able to be made available, unless it would be contrary to the public interest to do so. Access to data provided through a regulatory framework to facilitate its release and use is potentially valuable to government, the private sector and the community.

Opening up government data is consistent with, and an important part of Queensland's right to information 'push model'. OIC supports strategies and initiatives, such as Open Data, that maximise disclosure of government-held information to the community and provide appropriate protections for the community's personal information. Release of datasets under open government data initiatives is one mechanism for increasing transparency and accountability of government.

While publication of datasets is an important part of opening up government-held data for access and use, it does not replace the right to information (RTI) in Queensland. The RTI is broader than open data and includes other types of information such as reports, videos and

[1] Organisation for Economic Development (OECD), Open Government viewed at http://www.oecd.org/gov/open-government.htm

[2] Organisation for Economic Development (OECD), Trust in Government viewed at http://www.oecd.org/gov/trust-in-government.htm

audio recording. RTI provides a legal right to access government-held information not available administratively.

As noted in the Issues Paper, the amount of data being generated, collected and stored has been growing exponentially and 'by some estimates the amount of data generated worldwide in 2002 (five billion gigabytes) is now being generated every two days, while other estimates suggest that 90 per cent of the world's information was generated in just the past two years (IBM 2016)'.[3]

'Big data is seen today as the new opportunity for analytics that can offer significant advancements to several aspects of our everyday life, including health, leisure, environment, employments etc. To this end, data has been characterised by many as the fuel of the 21st century economy or the new oil'.[4] While greater data availability and use has the potential to deliver significant social and economic benefits, the rapid growth in the data being generated and the speed at which this data can be analysed has a number of implications for privacy and the protection of personal information.

As noted by the European Union Agency for Network and Information Security, 'the extensive collection and further processing of personal information in the context of big data analytics has given rise to serious privacy concerns especially relating to wide scale electronic surveillance, profiling and disclosure of private data'.[5]

Striking the right balance between greater data availability and use and the protection of an individual's privacy and personal data is critical to realising the benefits of data, achieving greater openness and transparency and enhanced levels of trust in government.

Privacy is often incorrectly cited as a barrier to enhanced data and information sharing by government agencies both within and external to government. Notwithstanding commonly-held misconceptions about privacy, OIC submits that a range of factors other than privacy prevent increased sharing of data and information by government including: risk-aversion; cultural and organisational factors; and legislated confidentiality provisions across a range of statutes. Further, not all datasets contain personal information and accordingly are not subject to the legislated privacy regime which is designed to provide the appropriate protections for only personal information.

In a recent study researchers noted that discussion needs to shift from 'big data versus privacy' to big data with privacy'[6] and that 'through careful planning and application of privacy techniques and principles, such as those embodied in Privacy-by-Design, organisations can use data for its business needs while at the same time protecting the personal information contained in the data'.[7] OIC submits that Privacy-by-Design and utilisation of privacy enhancing tools and techniques such as robust de-identification methods strike the right balance between data sharing and privacy.

RESPONSE

[3] Australian Government, Productivity Commission Issues Paper, Data Availability and Use, April 2016, p4

[4] European Union Agency for Network and Information Security, Privacy by design in big data, An overview of privacy enhancing technologies in the era of big data analytics, December 2015, p11 viewed at https://www.enisa.europa.eu/publications/big-data-protection

[5] See note 4 at p 5

[6] See note 4 at p 5

[7] Deloitte, Have it all – Protecting privacy in the age of analytics viewed at www2.deloitte.com/content/dam/Deloitte/ca/…/Analytics/ca-en-analytics-ipc-big-data.pdf

The Issues Paper raises a broad range of issues regarding data availability and use. This submission does not answer all questions raised in the Issues Paper. The OIC response predominantly focuses on addressing Privacy and Data Security issues raised in the Issues Paper.

In this context, OIC provides the following comments and suggestions for consideration:

CONSUMER ACCESS TO, AND CONTROL OVER, DATA

In Queensland, both the IP Act and the RTI Act create a right of access to documents, subject to certain exclusions and exceptions. The IP Act also provides an individual with a right of amendment of documents containing an individual's personal information.

The RTI Act gives a right of access to government information and intends that such information will be released administratively as a matter of course, unless there is a good reason not to. For example, where the information is private, confidential, legally privileged or subject to Cabinet confidentiality.

Open Data is an important part of proactive disclosure of government-held information and is consistent with Queensland public sector agencies' obligations under the RTI Act. The Queensland Government's Open Data Portal was launched in 2012 and currently has 2096 data sets available.[8] OIC submits that the value of Open Data is not measured by the number of data sets published but rather the accessibility, quality and value of the data published.

For example, publication schemes for proactively releasing key information about government agencies under the RTI Act require significant, appropriate and accurate information to be included in the scheme. In a Compliance Review of the Queensland Police Service a key recommendation was that "a full set of crime statistics, in a machine readable, reusable format, linked to geospatial information" be published in the publication scheme. Stakeholders consulted during the compliance review identified a number of different purposes to which such data could be applied. Crime data is now available in an interactive portal and raw data format, updated weekly.

Government agencies decide what datasets will be published and when this information will be made available potentially limiting consumer access to, and usefulness of, published datasets if the data made available is not what the community wants. OIC considers that effective engagement and consultation with the wider community about their information needs is critical to enhancing community access to data and reinforcing a culture of openness.

A key tenet of privacy is that individuals should be afforded choices and be able to exercise control in respect of their own information as far as practicable. OIC favourably notes the maxim 'When people have more control over their own data, more growth, innovation and value can be created than when they don't'.[9] OIC notes that some jurisdictions have sought to enact prescriptive regulatory frameworks that provide individuals with greater access to, and control over, data.

For example, the EU General Data Protection Regulation (the Regulation) provides a new data protection framework that strengthens the rights of individuals and increases the transparency of the processing. This includes a right to require information about data being

[8] https://data.qld.gov.au/

[9] Ctrl-Shift, A New Paradigm for Personal Data: Five Shifts To Drive Trust and Growth (June 2016) viewed at https://www.dropbox.com/s/2mpczioqti3h47m/Report%203%20A%20new%20paradigm%20for%20personal%20data.pdf?dl=0

processed about themselves, access to the data in certain circumstances, correction of data which is wrong and a clarified right to be forgotten. There is also a right to restrict certain processing and a right to object to their personal data being processed for direct marketing purposes.[10]

While OIC does not necessarily propose adopting the prescriptive regulatory approach of the EU, OIC submits that greater openness and transparency, including providing individuals with greater control over, and access to the data, is an important mechanism for building trust and confidence in government.

In an environment characterised by rapid technological change, 'the challenge for regulators is to 'build a flexible and responsive regulatory environment: one that focuses on developing trust in data practices, adapts quickly and effectively to emerging technologies, and creates a platform for positive practice to thrive'.[11]

OIC notes that the current legislative review of the IP Act by the Queensland Government may provide a more contemporary framework to manage emerging privacy risks and challenges posed by the rapid growth in technology.

PRIVACY PROTECTION

Queensland's Information Privacy Act 2009

In Queensland, the privacy principles in the IP Act set out how Queensland government agencies can collect, store, use or disclose personal information both within and outside Australia. Personal information is defined in the IP Act as 'information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.[12]

Government agencies include Ministers, Queensland Government departments, local government, Hospital and Health Services, public universities and other public authorities.[13] The IP Act does not apply to Government Owned Corporations (GOCs), individuals, the private sector or community organisations. Queensland GOCs, the private and community sector could be covered under the Commonwealth's privacy legislation if these entities have an annual turnover of more than $3 million per annum. Additionally, there is a measure of privacy protection in Queensland's Criminal Code and through the common laws of nuisance and trespass and in the area of recorded conversations.

Publishing personal information is a 'disclosure' and posting personal information online can result in the transfer of that information outside Australia.[14] The publishing of personal information specifically is potentially limited by the IP Act, particularly section 33 (overseas transfer) and Information Privacy Principle 11/National Privacy Principle 2.

---

[10] Allen & Overy LLP, the EU General Data Protection Regulation 2016, p7

[11] Ctrl-Shift, A New Paradigm for Personal Data: Five Shifts To Drive Trust and Growth (June 2016) viewed at https://www.dropbox.com/s/2mpczioqti3h47m/Report%203%20A%20new%20paradigm%20for%20personal%20data.pdf?dl=0 p12

[12] Section12

[13] The IP Act also applies to contractually bound service providers

[14] Disclosure is defined in section 23(2) IP Act.

The IP Act also allows an individual to make a complaint about an agency's breach of the privacy principles. If an individual – who need not be a Queensland citizen - considers that a Queensland Government agency has failed to comply with its obligations under the privacy principles, they are able to make a formal complaint.

While the IP Act provides the opportunity for the individual and the relevant government agency to settle the subject matter of the complaint between themselves, ultimately the privacy complaint can be referred to the Queensland Civil and Administrative Tribunal (QCAT) for its determination and orders. QCAT orders are remedial in nature; there is no capacity for it to order punitive measures.

There is the capacity for QCAT to award an individual up to a maximum of $100,000 in compensatory damages which can include non-economic loss.

In summary, Queensland has a statutory cause of action for privacy breach in respect of Queensland State Government agencies only.

The fact that a dataset contains personal information about individuals does not in itself prevent publication. The privacy breach arises when a dataset is published that contains information about an individual who can be identified using the data in the dataset and no exceptions apply. The dataset can be published once appropriate steps are taken to de-identify the data.

While it is acknowledged that combining datasets or 'mashing up' will realise the potential of open data, and that indeed, combination is inevitable in order to provide practical application of data, a degree of caution must be exercised because, however inadvertent, combination of datasets can lead to individuals being identified and consequently, their personal information being published. The 'mosaic effect' where seemingly innocuous datasets are combined to reveal significant and invariably unintended information is now a well-established phenomenon – see for example: https://gcn.com/articles/2014/05/14/fose-mosaic-effect.aspx

The well-publicised example of the then MIT undergraduate, Latanya Sweeney revealing of the medical information of Massachusetts Governor William Weld in 2010 serves as an illustration of the potential ease of re-identification from seemingly de-identified dataset – see http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

OIC acknowledges that the potential of re-identification is not readily apparent and 'given the development of increasingly powerful data sharing, matching and mining techniques – and a backdrop of strong political and commercial pressure to make more data available – it can seem inevitable that re-identification risk will increase exponentially'.[15]

Information regarding individual's health, location, electricity use, online activity…can be publicised, raising concerns about profiling, discrimination, exclusion and loss of control. OIC suggests that nonetheless, there is, as with open data generally, a balance that can be found between maximising publication and ensuring the privacy of individuals' whose information will be contained in the dataset remains protected.

How can individuals' and businesses' confidence and trust in the way data is used be maintained and enhanced?

[15] Elliot M, Mackey E, O'Hara K and Tudor C, 'the Anonymisation Decision Making Framework', University of Manchester 2016 p vii

As noted previously, OIC is of the view that openness and transparency is an important mechanism for building trust and confidence in government, including providing individuals with greater control over, and access to, their own data. Both the RTI and IP Acts in Queensland provide an individual with a legal right to access their own personal information and government held information, subject to limited exceptions.

In addition to greater openness and transparency about how data is used, some jurisdictions have found that adoption of robust data protection and data security mechanisms contributed to enhanced levels of trust in the way data is used.

For example, as noted previously, the EU General Data Protection Regulation (the Regulation) provides a new data protection framework that strengthens the rights of individuals and increase the transparency of the processing. These include a right to require information about data being processed about themselves, access to the data in certain circumstances, a right to restrict certain processing and a right to be informed when data security is breached.[16]

The Regulation also introduces a requirement for Privacy-by-Design and Privacy Impact Assessments.

What weight should be given to privacy protection relative to the benefits of greater data availability and use, particularly given the rate of change in the capabilities of technology?

'Big Data is, by its very nature, able to connect different data, which in itself would not be considered as personal data, but once aggregated, may lead to individuals being identified. 'This is a particularly challenging feature of Big Data as it may limit traditional de-identification methods; in this case, even anonymized data could be re-identified and attributed to an individual, which may create a data privacy breach.'[17]

A number of researchers and private sector organisations have noted that the 'idea of a trade-off between privacy and innovation is unhelpful and frankly outdated'[18] and advocate for shifting the discussion from 'Big Data versus Privacy' to 'Big Data with Privacy'.[19] Portraying that privacy is in conflict with greater data availability and use contributes to the perception by government agencies that privacy is a barrier to publication of data.

OIC submits that adoption of Privacy-by-Design, a framework for embedding privacy measures and privacy enhancing technologies directly into the design of information technologies and systems, 'supports innovation without compromising personal information'.[20] 'Privacy-by-design has become the international privacy standard. Further the United Nations,

[16] Allen & Overy LLP, the EU General Data Protection Regulation 2016, p7

[17] Big Data, Big Brother? Striking the right balance with privacy, Deloitte, viewed at https://www2.deloitte.com/content/dam/.../lu/.../lu_en_**big**-**data**-**big**-brother_122015.pdf

[18] Deloitte, Have it all: Protecting privacy in the age of analytics, https://www2.**deloitte**.com/content/dam/**Deloitt e**/.../ZA_**Privacy**bydesign_270515.pdf

[19] enisa, European Union Agency for Network and Information Security, Privacy by design in big data viewed at https://www.enisa.europa.eu/publications/beig-data-protection

[20] Deloitte, Have it all: Protecting privacy in the age of analytics, https://www2.**deloitte**.com/content/dam/**Deloitt e**/.../ZA_**Privacy**bydesign_270515.pdf p6

the European Parliament and the US government have indicated that Privacy-by-Design is absolutely critical in maintaining personal privacy'.[21]

OIC notes that while rapid growth in technology poses a number of number of privacy challenges, particularly in respect of Big Data, this same technology offers a range of opportunities with regards to privacy protection. The UK Information Commissioner recently commented that 'it is essential that we continue to develop anonymization and other privacy enhancing techniques as an antidote to the potential excesses of the big data era'.[22]

OIC has been actively involved in providing expert privacy advice to agencies since the Open Data initiative was launched in Queensland in 2012. A considerable part of our role has been to dispel myths and provide clear advice regarding how datasets can be released, and what the actual restrictions are as they are often legislative confidentiality requirements specific to the agency's functions. Providing clarity about what can be achieved in a privacy respectful approach to sharing data to promote greater use and openness, has shown that a Privacy-by-Design approach is preferable and can be more effective for all objectives.

Strong leadership within agencies is also critical to successful changes to how agencies use data. It is clear that culture is important and people feel strongly about their responsibilities as custodians of data and need clear direction when expectations changes about opening up data that was previously closed to others.

The benefits of sharing data have been well documented and have also been the subject of work conducted as part of a partnership between OIC and the Australian and New Zealand School of Government Transparency Occasional Paper Series. These papers consider performance data, opening up data for productivity and greater transparency and accountability, including the United Kingdom experience. The papers can be accessed at:

https://www.oic.qld.gov.au/publications/research/transparency-occasional-paper-series

Are further changes to the privacy-related policy framework needed? What are these specific changes and how would they improve outcomes? Have such approaches been tried in other jurisdictions?

OIC recognises that the rapid growth in the technology and the ease with which 'personal information' can be obtained, used and disseminated has exposed individuals to new privacy risks or exacerbated existing risks to the point where the adequacy of existing protections requires consideration.

For example, ensuring personal data protection becomes more challenging as information is multiplied and shared even more widely around the world. In this context, OIC notes that 'current privacy regulatory regimes may not be enough to address privacy issues in digital ecosystems where data flows across regions and continents'[23] As noted by Priscilla Guo in the Harvard Political Review[24], 'with data untied to any physical location, the laws governing said data must be similarly expansive'.[25]

---

[21] EY, Building on the Key Trends, http://www.ey.com/GL/en/Services/Advisory/ey-building-on-the-key-trends

[22] T Elliot M, Mackey E, O'Hara K and Tudor C, 'the Anonymisation Decision Making Framework', University of Manchester 2016

[23] EY, Building on the key trends, Can privacy really be protected anymore? viewed at http://www.ey.com/GL/en/Services/Advisory/ey-building-on-the-key-trends

[24] Guo, P, No More Safe Harbour, Harvard Political Review, viewed at http://harvardpolitics.com/world/no-more-safe-harbor/

[25] viewed at http://harvardpolitics.com/world/no-more-safe-harbor/

In general terms, there is no privacy law in Queensland that applies to acts of privacy breach by individuals, small business or small community sector organisations. Nor does the IP Act apply to Government Owned Corporation (GOCs).[26] Queensland GOCs, the private and community sector could be covered under the Commonwealth's privacy legislation if these entities have an annual turnover of more than $3 million per annum.

Other Jurisdictions

OIC notes that international jurisdictions have broader applicability of privacy legislation. For example, New Zealand's *Privacy Act 1993* applies to any person or body of persons, whether corporate of unincorporated, and whether in the public or private sector. Organisations not covered by the Privacy Act are limited to members of Parliament, courts and tribunals in relation to their judicial functions and the news media when they are conducting their news activities.

Canadian privacy legislation is framed around Canada's private and public sector. The *Personal Information Protection and Electronic Documents Act* applies to all organisations that collect, use or disclose personal information in the course of their commercial activities, except those provinces which have enacted legislation that is deemed to be substantially similar. Public bodies that operate in Canada's public sector, such as educational, health care and local government bodies are subject to Canada's *Privacy Act.*

In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU to take into account vast technology changes of the last 20 years'.[27] On 14 April 2016 the Regulation and the Directive were adopted by the European Parliament to standardise data privacy laws across the EU. Device makers will have stricter requirements to build data protection into their devices from the very beginning of the design process.[28]

'The changes under the EU regulation will provide a person with more control over their personal data and make it easier to access it. 'They are designed to make sure that people's personal information is protected – no matter where it is sent, processed or stored – even outside the EU'.[29] The EU regulatory framework includes:

- a right to be forgotten – when an individual no longer wants her/his data to be processed, and provided that there are no legitimate grounds for retaining it, the data will be deleted.
- mandatory data breach notification
- 'Privacy-by-Design' or Data Protection by Design and by default – building data protection safeguards into products and services from the earliest stage of development
- stronger enforcement powers[30] and
- promotion of anonymization, pseudonymization and encryption to protect personal data.[31]

[26] The IP Act also applies to contractually bounds contracted service providers

[27] Hawthorn N, 10 things you need to know about the new UE data protection regulation, viewed at http://www.computerworlduk.com/security/10-things-you-need-know-about-new-eu-data-protection-regulation-3610851/

[28] http://www.zdnet.com/article/privacy-laws-how-the-us-eu-and-others-protect-iot-data-or-dont/

[29] http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

[30] http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

[31] http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

A US Federal Trade Commission proposed a privacy-related policy framework with three main recommendations: Privacy-by-Design, giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency of data practices.[32]

OIC considers any policy or legislative privacy-related framework needs to be sufficiently flexible to adapt to ongoing technological change, the components of which may include:

- 'Privacy-by-Design
- mandatory data breach notification
- Providing agencies with a range of privacy enhancing tools, such as de-identification, to enable robust de-identification of datasets. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing and publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information while protecting privacy'[33]
- user access controls
- greater transparency and openness

As noted by researchers, Big Data in particular poses significant challenges for the protection of personal sensitive information and 'as a result, privacy preservation simply cannot be accomplished by de-identification alone' and propose the 'privacy by design paradigm to develop technological frameworks for countering the threats of undesirable, unlawful effects of privacy violation, without obstructing the knowledge discovery opportunities of social mining and big data analytical technologies.[34]

COLLECTION AND RELEASE OF PUBLIC SECTOR DATA

What criteria and decision-making tools do government agencies use to decide which public sector data to make publicly available and how much processing to undertake before it is released?

Queensland government agencies hold large amounts of information about Queensland and the community. There are a number of laws which apply to this information, including the RTI Act, the IP Act and the *Public Records Act 2002* (Qld).

Queensland's IP Act and the RTI Act give a right of access to information in the government's possession or under the government's control unless, on balance, it is contrary to public interest to give the access. Government information should, where possible, be given through informal means like an agency's website, publication scheme, or through administrative release. A formal application for government-held information under the RTI Act or IP Act should only be made as a last resort. The Queensland Government Open Data Portal facilitates government agencies publishing datasets and information holdings on an ongoing basis.

Significant and appropriate information should be included in an agency's publication scheme, which can be achieved through linking to the data portal where applicable. Performance information is of considerable interest to the community and is important in relation to an

[32] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for businesses and policymakers, March 2012 p1

[33] Garfinkel, S L De-Identification of Personal Information, National Institute of Standards and Technology, U.S. Department of Commerce, p iii

[34] DPJ Data Science, Privacy-by-design in big data analytics and social mining viewed at https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-014-0010-4

agency's accountability and transparency. Government should engage with the community to ask what information is of interest and important to release. Stakeholder consultation during OIC performance monitoring reviews has shown that it is not always apparent to an agency the purposes to which its' data can be applied. Such consultation can also assist in determining the priority to be given to particular datasets.

Both the RTI Act and IP Act allow people to apply for documents containing information. Document is not defined in the RTI Act. However, schedule 1 of the *Acts Interpretation Act 1954 (*Qld) provides that a document includes paper or other material or meaningful marks, symbols or figures on it, and any disc, tape or other article from which images, writing or messages can be produced.

Both Acts set out a public interest balancing test which sets out how competing public interest factors should be compared and considered when making a decision about whether to allow or refuse access to the information. For example, Schedule 4 of the RTI Act outlines a non-exhaustive list of factors the Parliament considers relevant to determining whether the disclosure of information would, on balance, be contrary to the public interest.

Many datasets held by government contain personal information. This personal information must be protected in the way set out in the IP Act and the privacy of individuals taken into account when publishing data. The dataset can be published one appropriate steps are taken to de-identify the data so that individuals are no longer apparent, or reasonably ascertainable, from the data. Once information is appropriately de-identified it is no longer personal information, but the risk of re-identification should be considered as part of the decision to publish a dataset.

The IP Act requires special protections to be given to sensitive information in the area of health services.[35] Where datasets contain sensitive or other personally significant information, health agencies may wish to take that into consideration as part of their privacy risk assessment.

Sensitive information is information concerning an individual's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual preferences or practices
- criminal record
- health information.

OIC has published guidelines on its website regarding publication and privacy. The guidelines can be accessed at:

[35] These requirements apply only to health agencies; see National Privacy Principle 9.

https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/dataset-publication-and-privacy

https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/dataset-publication-and-risk-assessment

https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/proactive-disclosure/dataset-publication-and-de-identification-techniques

DATA SECURITY

How should the risks and consequences of public sector and private sector data breaches be assessed and managed? Is data breach notification an appropriate and sufficient response?

OIC recently provided a submission to the Australian Government's Serious Data Breach Notification Consultation which closed on 4 March 2016. In this submission, OIC provided in principle support for a legislated mandatory data breach notification scheme by the Australian Government. OIC noted that the introduction of a mandatory data breach notification scheme serves to strengthen the existing regulatory framework and brings Australia in line with other jurisdictions, including the EU, the United Kingdom and the Unites States.

In addition to allowing affected individuals to take remedial steps to less the adverse consequences that may arise from a data breach, data breach notification is an important transparency measure for governments. Governments collect and hold vast amounts of personal information on behalf of its citizens and citizens trust that Governments will protect this information from unauthorised access, use and disclosure. Increasingly, this information is held digitally posing significant implications for an individual's privacy in the event of a data breach.

Openness and transparency is an important mechanism for building trust and confidence in government. Given the significant economic and reputational costs associated with data breaches, it is OIC's view that entities may be reluctant to report data breaches unless mandated to do so.

Queensland's privacy principles include obligations which require agencies (and bound contracted service providers) to protect the information they hold from misuse, loss, and from unauthorised access, modification or disclosure. The IP Act also obliges agencies to safeguard the privacy of personal information when transferring information out of Australia. However, the IP Act does not require agencies to notify either affected individuals or the Information Commissioner of a privacy breach.

Queensland State Government agencies have obligations to report information security incidents to the Queensland Government Chief Information Officer as part of the IS18 Information security incident reporting requirements.

OIC also encourages agencies under the IP Act to incorporate data breach notification into its information management processes as a responsible business practice and to communicate with the Queensland Privacy Commissioner when incidents of data breach occur.

To date, only a small number of Queensland State Government agencies and their contracted service providers have reported data breach notifications to the OIC. However, in the absence of reliable data and a legislative framework mandatory reporting of data breaches, it is difficult to state with any certainty the actual number of data breaches in Queensland.