Submission No 14

INQUIRY INTO CYBERSECURITY

Organisation: Information and Privacy Commission NSW

Date Received: 18 September 2020

information and privacy commission new south wales

Enquiries: Jessica Kavanagh

Our reference: IPC20/A000311

18 September 2020

The Hon Tara Moriarty MLC
Committee Chair
Portfolio Committee No. 1
NSW Legislative Council
Parliament of New South Wales

By email: PortfolioCommittee1@parliament.nsw.gov.au

Dear Ms Moriarty

INQUIRY INTO CYBERSECURITY

The purpose of this correspondence is to provide a submission to the Portfolio Committee 1 – Premier and Finance Inquiry into Cybersecurity.

The following comments are provided to assist the Committee in its consideration of this important issue.

About the IPC

The Information and Privacy Commission NSW (IPC) oversees the operation of privacy and information access laws in New South Wales.

The Privacy Commissioner has responsibility for overseeing and advising NSW public sector agencies on compliance with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

The Information Commissioner has responsibility for overseeing the information access rights enshrined in the *Government Information Public Access Act 2009* (GIPA Act).[1] These rights are realised by agencies authorising and encouraging proactive public release of government information; and by giving members of the public an enforceable right to access government information.

Impact of cyber threats

The NSW Government has led the way in development of digital government and the implementation of new and innovative service delivery for its citizens. As the range of services available via digital platforms expands, so to do the threats and risks to the security of these services and the data holdings of government. As the NSW Government continues to implement its digital transformation agenda, including the use of artificial intelligence and automated decision-making, maintaining and enhancing the cyber security capabilities of the public sector is vital to protecting the security of its information assets.

[1] The functions of the Privacy Commissioner and the Information Commissioner are set out in a fact sheet about the IPC's functions.

The Information and Privacy Commission is playing a leading role in expanding the capabilities of the NSW public sector through the production of resources including statutory guidance, fact sheets and importantly the regular provision of advice to agencies and citizens regarding the preservation and exercise of rights in digital government. The IPC's work volumes have increased significantly in response to the NSW Government's Digital Government Strategy released in early 2017. Between 2015/16 and 2019/20 requests to the IPC for advice have increased by 171%.

Cyber security threats can take a variety of forms including crypto-mining, data breaches, distributed denial of service (DoS) attacks, hacking, identity theft, malware, ransomware, web shell malware, phishing attacks and spoofing.[2] In addition to these various and ever evolving digital threats, human error and lack of training in cyber security awareness also pose a significant risk. It has been suggested that "as many as 95% of successful online hacks come down to human error". [3]

The Australian Cyber Security Centre (ACSC) reported in its December 2019 *Cyber Crime in Australia* that it received 13,672 reports of cybercrime between July and September 2019. "This equates to an average of 148 reports per day, or one every 10 minutes. Of these 13,672 reports, 11,461 contained sufficient information to be referred to state and territory law enforcement agencies."[4] The ACSC also reported the impacts of cybercrime for individuals and business, with:

- average financial loss per report of $6,000,
- more than $890,000 in reported losses each day,
- annual estimated losses to cybercrime of $328 million.

Privacy

A strong cyber security environment is an essential pre-condition to the building and maintenance of robust and privacy protective information governance systems. As governments move forward with the digital transformation agenda the importance of a sustained focus on cyber security and privacy protection cannot be underestimated.

The PPIP Act and HRIP Act establish the Information Protection Principles and Health Privacy Principles which govern the collection, use and disclosure of personal and health information by NSW government agencies and, in the case of the HRIP Act, private sector health care providers.

Section 12 of the PPIP Act specifically imposes an obligation on NSW public sector agencies to ensure that personal "information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse …".

The appropriate level of security that may be required in relation to personal information will depend on both the nature of the information and the medium in which it is stored. What is 'reasonable' will differ depending on the circumstances and can include:

- physical safeguards such as locking filing cabinets and positioning computer screens so they cannot be seen by the public,
- administrative safeguards such as appropriate policies, procedures and staff training,
- technical safeguards such as password-protected databases, secure transmission, encryption, two factor authentication and electronic audit trails.

[2] Australian Cyber Security Centre

[3] Swivelsecure

[4] Australian Cyber Security Centre, *Cyber Crime in Australia,* (December 2019), p5.

Data Breach

Data breaches are a matter of significant concern to the IPC. With governments providing an ever-greater range of services via digital platforms, the amount of digital information held by government is growing at an exponential rate. This presents a highly valuable target for malicious actors.

As demonstrated by the most recent data released by the Office of the Australian Information Commissioner (OAIC), sixty five percent of data breach notifications received by the OAIC between January and June 2020 were the result of malicious or criminal attacks. Most of these were attributable to incidents resulting from common cyber threats such as phishing, compromised or stolen credentials, ransomware or other forms of hacking. Thirty four percent of breaches were attributable to human error, with system faults accounting for the remaining five percent of reported breaches.[5]

While NSW does not currently operate a mandatory data breach reporting scheme, the Privacy Commissioner strongly encourages NSW public sector agencies to report data breaches under the voluntary reporting scheme.

A data breach occurs when there is a failure that has caused or has the potential to cause unauthorised access to an agency's data. Although malware, hacking and data theft are usually the first examples of data breaches that come to mind, many breaches are a result of simple human or technical errors rather than malicious intent. The accidental loss of a paper record, laptop, or USB stick may constitute a data breach, as would emails sent to the wrong recipients if they contained classified material or personal information. Data breaches can also occur if authorised system users access restricted information for unauthorised reasons, such as employees looking up agency-held information for personal reasons.

Some data breaches are serious and can potentially harm individuals and agencies whose information is breached. The current voluntary scheme encourages agencies that have experienced a serious data breach to report the details of the breach to the Privacy Commissioner, so that the Privacy Commissioner can assess the breach, provide advice or investigate. Agencies are also encouraged to voluntarily notify people affected by a data breach and provide information about their right to seek an internal review under the PPIP Act in relation to the breach.

The impact of a data breach depends on the nature and extent of the breach and the type of information that has been compromised. Some breaches may involve only one or two people while others may affect hundreds or thousands. Larger breaches expose a wider group of people to potential harm and could require considerable notification and remediation activities. However, it is not only the initial size of the breach that determines its impact. If there is a breach of sensitive or confidential information, reputational and financial harm can occur for the agency itself, agency staff, as well as the Government.

Breaches of personal data can result in significant harm, including people having their identities stolen or the private home addresses of protected or vulnerable people being disclosed. As such, even a breach affecting a small number of people may have a large impact.

In 2018, the Privacy Commissioner commenced the quarterly reporting of voluntary data breaches notifications received from agencies. During the reporting year 2019/20 the Privacy Commissioner received a total of 79 breach notifications, which represents an increase of 23 per cent over the previous year. This data can be accessed on the IPC website. The IPC has also provided public sector agencies with resources to assist them to manage and respond to a data breach incident. This includes a data breach guidance, notification forms and a prevention checklist.

[5] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2020/

The IPC engages with agencies that have experienced a serious data breach and provides comprehensive advice to agencies to assist them to improve their privacy and information governance policies, procedures and practices. In 2019/20 the IPC engaged with a number of agencies including:

- Revenue NSW in relation to their systems and practices following a data breach,
- Service NSW in relation to a cyber related data breach,
- Revenue NSW on the implementation of the mandatory notification requirements required by the *Fines Amendment Act 2019.*

The IPC has undertaken extensive consultation with the Department of Communities and Justice, the Department of Customer Service and the NSW Ministry of Health on the development of a draft model for a mandatory reporting scheme in NSW. The Privacy Commissioner supports the development of a mandatory data beach notification scheme which includes a requirement to notify both the Privacy Commissioner and the affected individuals where a data breach results in, or is likely to result in, a serious risk of harm to the individual.

Privacy by Design

The Privacy Commissioner encourages NSW public sector agencies to take a proactive 'privacy-by-design' approach to all digital programs and projects. Privacy by Design (PbD) is a specific approach to privacy, developed by Dr Ann Cavoukian, the former Privacy and Information Commissioner of Ontario, Canada, in the 1990s.

The PbD framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010. The U.S. Federal Trade Commission recognised PbD in 2012 as one of its three recommended practices for protecting online privacy in its report entitled, *Protecting Consumer Privacy in an Era of Rapid Change*. More recently, PbD has been incorporated into article 25 of the *European Union General Data Protection Regulation*.

Privacy by Design is a methodology that enables privacy to be built into the design and structure of information systems, business processes and networked infrastructure. PbD considers privacy and security requirements from the outset. Implementing preventative measures which remove or mitigate privacy and security risks is more effective to containing costs, managing community expectation and realising policy intent than developing legislative exceptions to privacy laws or redesigning programs or digital solutions after the fact.

Privacy by Design aims to ensure that privacy is considered at all stages of the project life cycle from conception through to development and implementation of initiatives that involve the collection and handling of personal information. It positions privacy as an essential design feature of public sector practices and shifts the privacy focus to prevention rather than compliance.

The Privacy by Design methodology is built around seven foundational principles:

- **Proactive not reactive, preventative not remedial:** The PbD framework is characterised by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy-invasive events before they occur.
- **Privacy as a default setting:** PbD seeks to deliver the maximum degree of privacy by ensuring that personal information is automatically protected in any given IT system or business practice, as the default.
- **Privacy embedded into design:** Privacy measures are embedded into the design and architecture of IT systems and business practices. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system, without diminishing functionality.

- **Full functionality: positive-sum not zero-sum:** PbD seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a zero-sum (either/or) approach, where unnecessary trade-offs are made. PbD avoids false dichotomies, such as privacy versus security, demonstrating that it is indeed possible to have both.
- **End-to-end security – full lifecycle protection:** PbD extends securely throughout the entire lifecycle of the information involved. This ensures that all information is securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion.
- **Visibility and transparency – keep it open:** PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is operating according to the stated promises and objectives, subject to independent verification. The individual is made fully aware of the personal information being collected, and for what purposes. All the component parts and operations remain visible and transparent, to users and providers alike.
- **Respect for user privacy – keep it user centric:** PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Privacy Impact Assessment

Tools such as Privacy Impact Assessments (PIAs) are valuable in assisting public and private organisations in managing privacy and security risks. A PIA is a systematic assessment of a project which identifies the impact that the project may have on the privacy of individuals and sets out a process or recommendations in addressing this risk.

PIAs are more than a 'compliance check' against privacy legislation. Critically, PIAs allow data custodians to gain an insight into information flows within their organisation, demonstrate corporate responsibility and provide the community with the confidence that a proposed project accords with community expectations towards privacy, data security and appropriate information management. It enhances the quality of information available to decision makers and demonstrates that a project has been designed with privacy in mind.

The timing of a PIA is crucial. A PIA should be conducted early enough so that it can genuinely affect project design, yet not too early as to prevent an agency from obtaining the necessary information about the project to adequately assess any privacy risks.

There are seven key elements to achieve an effective PIA, namely:

- **Integral to an organisation's governance:** the PIA should be integrated into an organisation's governance structure and have clear guidance on who has responsibility over the PIA;
- **Fit for purpose:** the PIA should be commensurate with the potential privacy risks associated with the project;
- **Comprehensive:** the PIA should cover all privacy issues, not just information privacy. A PIA should also consider whether change is required in supporting documentation such as Privacy Management Plans, human resource policies or training material to accompany project implementation;
- **Available:** the PIA report should be publicly accessible as this demonstrates accountability. Where this is not possible, consider releasing a PIA summary report to notify and seek feedback on privacy issues;
- **Enables compliance:** the PIA must address all legal obligations, including under privacy legislation, namely, the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) where relevant;
- **Ongoing:** the PIA should contain an ongoing review mechanism to assess privacy issues throughout the life cycle of the project; and

- **Constructive:** the PIA should support an organisation's privacy culture and reference the organisation's risk management process.

Data Sharing

Data sharing is another area where appropriate cyber security is a significant factor in ensuring that agencies are compliant with their privacy obligations. As agencies continue to share ever increasing quantities of personal and non-personal data with other government agencies and non-government organisations, ensuring that these partners have in place commensurate levels of cyber security protections will be vital.

The IPC has recently published guidance for NSW public sector agencies on safe and privacy respectful data sharing, including advice on the need to ensure that the receiving agency has appropriate levels of security to safeguard any data provided.

Engagement with Cyber Security NSW

In 2020, the Privacy Commissioner entered into a formal information sharing protocol with Cyber Security NSW to facilitate the sharing of information for the purpose of discharging the Privacy Commissioner's functions under the PPIP Act.

The IPC regularly engages with Cyber Security NSW on matters of common interest.

Privacy Awareness Week 2020

The IPC engages proactively with agencies to highlight the importance of good privacy practice, including privacy risks that need to be mitigated, such as cyber-security risks.

Privacy Awareness Week was held from 4 – 10 May 2020 with the theme **Prevent, Detect, Protect**. The campaign engaged both public sector agencies and citizens to assist in improving understanding and awareness of NSW privacy legislation and raising awareness of NSW privacy rights and agency obligations.

The NSW Privacy Commissioner launched Privacy Awareness Week NSW 2020 at the online Public Sector Forum in Sydney. The Forum was opened by the Attorney General and Minister for the Prevention of Domestic Violence, Mark Speakman. The keynote speaker at the event was Professor Lacey from IDCare. IDCare is a not-for-profit Australian charity formed to provide support for individuals affected by identify theft and cyber security concerns.

Professor Lacey presented on misuse of personal information in NSW, and Tony Chapman, Chief Cyber Security Officer at Cyber Security NSW answered questions from the Privacy Commissioner on NSW cyber security and NSW government initiatives.

Information Access

As government increasingly adopts digital technology it has a duty to implement administrative practices that safeguard the legislated commitment to open government and the fundamental right of access by citizens to government information. Digital government necessitates adapting existing practices to the digital environment to future proof the right to access information. Robust cyber security policies and settings contribute to safeguarding the integrity of information held by government. Safeguarding that information also recognises the imperatives under the GIPA Act.

Object of the GIPA Act

The object of the GIPA Act is to open government information to the public and in doing so maintain and advance a system of responsible and effective representative democratic government that is open, accountable, fair and effective. This object is to be realised by agencies authorising and encouraging proactive public release of government information (section 3(1)(a)); and by giving members of the public an enforceable right to access to government information (section 3(1)(b)).

Subsection (1)(c) under section 3 of the GIPA Act provides that access to government information is restricted only when there is an overriding public interest against disclosure.

It is the intention of Parliament that the GIPA Act be interpreted and applied so as to further its object (section 3(2)(a)); and that the discretions conferred by the GIPA Act be exercised, as far as possible, so as to facilitate and encourage, promptly and at the lowest reasonable cost, access to government information (section 3(2)(b)).

What is a government record?

Section 4 of the GIPA Act defines government information as information contained in a record held by an agency.

Under the GIPA Act a record includes any document or other source of information compiled, recorded or stored in written form or by electronic process, or by any other manner or by any other means.[6] This means that in addition to paper or hard copy records, digital records can be the subject of a GIPA application, where that information is held by the agency.

The *State Records Act 1998* also defines record as any document or other source of information compiled, recorded or stored in written form or on film, or by electronic process, or in any other manner or by any other means.[7] Additionally, the State Records Act also defines a record in relation to its official nature, not just how it has been created or stored. The Act defines *state records* as those records which are made and kept, or received and kept …in the course of the exercise of official functions.[8] This means that any information created or received in the course of an officer's duties as a public servant, regardless of format or the technologies used, are records and must be managed in accordance with the State Records Act.

Any Government information that is compiled, recorded or stored in a digital format or in a digital platform may be considered a record, including:

- SMS messages on a mobile phone;
- messages in WhatsApp;
- emails and any attachments;
- electronic copies of documents (including draft documents);
- contents within a database (such as a record or data in a business system or online application or software-as-a-service application);
- audit and access logs for business systems; and
- CCTV footage and other audio-visual information.

Increasingly, agencies are utilising new technologies and digital platforms to carry out their business or in providing services to the public. For example, many agencies use a range of new digital platforms (including Twitter, Yammer and Microsoft Teams) as part of their business. Agencies should be aware that messages, forums and posts created using these platforms are digital records under the GIPA Act if they have been used for conducting government business. Similarly, messages created in messaging apps (such as WhatsApp, Facebook Messenger and WeChat) are digital records if the messages have been used for conducting government business.

[6] GIPA Act clause 10 of Schedule 4

[7] State Records Act section 3, definition of a record

[8] ibid

If an agency uses these technologies to conduct business within the agency or externally with clients etc, then the agency is creating digital records within these systems. The agency will need to determine how it will capture and store these records and make them available if required under the GIPA Act. It is important that agencies have in place systems and governance arrangements that communicate to staff expectations and responsibilities associated with the use of these technologies under the GIPA Act. Under the State Records Act agencies have a responsibility to ensure safe custody and proper preservation of State records under their control.[9]

The IPC has published guidance on digital records and GIPA Act to assist agencies with the development and maintenance of good digital recordkeeping practices to ensure they are able to comply with their legislative obligations.

When is information held by a government agency?

Information is held by an agency when it is:

- information contained in record held by an agency,
- information contained in a record held by a private sector entity to which the agency has an immediate right of access,
- information contained in a record in the possession or custody of the State Records Authority to which the agency has an immediate right of access,
- information contained in a record that is in the possession or under the control of a person in his or her capacity as an officer or member of staff of an agency.[10]

Under the GIPA Act an agency must have an agency information guide which identifies the various kinds of information held by the agency (section 20(1)(d)). The guide must be made publicly available, together with an agency's policy documents (sections 6, 18(a) and 18(c)). What constitutes an agency's policy documents is set out in section 23 of the GIPA Act.

Section 23 of the GIPA Act may have particular application to government policies relevant to the management and exchange of data. Section 23 provides:

> *An agency's policy documents are such of the following documents as are used by the agency in connection with the exercise of those functions of the agency that affect or are likely to affect rights, privileges or other benefits, or obligations, penalties or other detriments, to which members of the public are or may become entitled, eligible, liable or subject (but does not include a legislative instrument)—*
>
> *(a) a document containing interpretations, rules, guidelines, statements of policy, practices or precedents,*
>
> *(b) a document containing particulars of any administrative scheme,*
>
> *(c) a document containing a statement of the manner, or intended manner, of administration of any legislative instrument or administrative scheme,*
>
> *(d) a document describing the procedures to be followed in investigating any contravention or possible contravention of any legislative instrument or administrative scheme,*
>
> *(e) any other document of a similar kind.*

In the context of digital government public awareness and public trust will be enhanced by transparency of government policies that impact citizens who share their information with government. Public confidence is more readily secured by provision of information that enables citizens to understand the government's commitment and approach to combatting cyber threats and securely managing data.

---

[9] State Records Act section 11(1)

[10] GIPA Act, clause 12 of Schedule 4

Community expectations

In 2020 the IPC has continued to build upon the research initiated in 2014 regarding community attitudes to the right to access information. In 2018 and 2020 the survey explored community attitudes to government's use of data.

In 2020 the results of the survey confirmed that:

- 88% of citizens felt that their right to access government information was important.
- 72% agreed that de-identified information should be used to inform planning and service delivery.
- 81% agreed that agencies should publicly report on the information they maintain.
- 78% agreed that agencies should publicly report on the use of machine learning to enhance decision making.

These results also call for accountability by government with and a compelling case for 'future proofing information access rights' and ensuring that information in whatever form is available for access. The full results of the 2020 survey will be released during Right to Know Week 2020 and will be available on the IPC website.

Reasonable search requirements

In responding to an access application, agencies are required to undertake a reasonable search for information requested. What constitutes a reasonable search will depend on the circumstances. Specifically, the requirements are that an agency:

- must have undertaken such reasonable searches as necessary to locate the government information requested;
- must use the most efficient means reasonably available to it; and
- only needs to search for government information held at the time of the application.

The expression "government information" is given a wide meaning by section 4 of the GIPA Act. This means that searches will need to be broadly conducted and include both paper-based and electronic records. Agencies are not required to search their backup or archive systems unless the government information requested has been improperly destroyed or transferred.

Searches should be conducted in a comprehensive manner. This may involve backend and metadata searches using information technology expertise. The use of electronic data management systems should facilitate faster and more effective search processes resulting in lower processing charges for applicants.

Agencies are encouraged to provide certification and attestation in relation to information access searches particularly where specialist expertise is required. This should include identifying:

- search terms applied,
- systems searched,
- information identified,
- officer conducting the search return to the GIPA access application decision-maker by way of certification or attestation e.g. signature or other identification.

Agency Information Guides

Under Part 3 Division 2 of the GIPA Act all agencies (except Ministers) are required to publish an agency information guide (AIG) This document is required to describe:

- an agency's structure,
- functions,

- how those functions, including, in particular, the decision-making functions of the agency affect members of the public,
- the type of information held by the agency and how it is made publicly available.

Pro-integrity features of the GIPA Act

The GIPA Act is technology neutral and applies to all government information regardless of the format in which it is held. This ensures that information access rights are maintained as government implements new forms of technology to deliver services and protect against cybersecurity threats.

The guiding principle of the GIPA Act is to make information more accessible to the public. The GIPA Act embodies the general presumption that the disclosure of information is in the public interest unless there is a strong case to the contrary.

This places the GIPA Act at the centre of the endeavour to achieve transparency and integrity in government.

The right to access information and independent oversight of that right is recognised as a core feature of a healthy pro-integrity system. Within NSW the GIPA Act and the *Government Information (Information Commissioner) Act 2009* (GIIC) operate to achieve pro-integrity outcomes through both *ex ante* and *ex post* disclosure mechanisms including:

- Mandating proactive disclosure of government information such as agency information guides, policy documents, and government contracts (Part 3 Open access information).
- Providing avenues for redress including investigation of complaints regarding the exercise of information access functions and review rights in respect of information access decisions.
- Offence provisions that address unlawful behaviour in relation to deciding access application and handling of government information; in particular, section 120 which makes it an offence to conceal or destroy government information.

Preservation of the principles of open government under significant government partnership and outsourcing arrangements

Technology is a recognised enabler for the delivery of more accessible, effective and often lower-cost services. It is also recognised as an effective tool in combatting corruption as it enables ready access to information and audit mechanisms. Accordingly, in the government context technology should promote and enable faster, more effective and lower cost access to information. New South Wales is at the forefront of initiatives to harness the benefits of technology and data to provide excellence in public services. The increasing adoption of technology demands the preservation, assurance and assertion of information access rights.

The domain of government service delivery is increasingly contested. Importantly, the GIPA Act recognises that citizens' rights do not diminish under these arrangements. Accordingly, there is increasing demand for the preservation of accountability, transparency, and citizen engagement within these arrangements particularly those harnessing digital innovation.

These outcomes can be achieved through express contractual provisions that secure the right to access information including enhanced mandatory contract reporting and additional open access information requirements.

Government information held by third parties

The Information Commissioner expects agencies to have regard to the application of section 121 of the GIPA Act when entering into contracts with private sector persons to ensure that certain information held by contractors is designated as government information and subject to the GIPA Act.

A reference in the GIPA Act to government information held by an agency is a reference to information contained in a record held by a private sector entity to which the agency has an immediate right of access (clause 12(1)(b) of Schedule 4 to the GIPA Act). Section 121 of the GIPA Act contains mandatory requirements for certain government contracts to provide for immediate rights of access to information held by private sector contractors.

Where such contractual rights exist, an access application under section 9 of the GIPA Act can be made to the agency for that information, and a person has a legally enforceable right to be provided with access to the information in accordance with Part 4 of the GIPA Act unless there is an overriding public interest against disclosure of the information.

Section 121 of the GIPA Act applies in circumstances where an agency enters into a contract with a private sector entity to provide services to the public on behalf of the agency.

Subject to certain exceptions, section 121 requires government agencies to ensure that their contracts provide them with an immediate right of access to information:

- relating directly to the performance of services by the contractor,
- that is collected by the contractor from members of the public to whom it provides, or offers to provide, the services, and
- that is received by the contractor from the agency to enable the contractor to provide the services.

Section 121 mandates the inclusion of a clause to permit access to information held by the contractor. Despite the mandatory requirements of section 121, where there are no contractual arrangements in place and no immediate right of access to information, information in the possession of a contractor may not be government information held by an agency for the purposes of the GIPA Act.

Rights promotion

As NSW public sector agencies are increasingly using data and adopting new technologies to more efficiently and effectively deliver systems to the public more information is held in digital form. Digital information takes many forms for example source codes, test suites, algorithms, and CCTV footage. It is essential that this information is held securely to preserve the right to access information and enable citizens to exercise their right of access.

The right of access to information is an enabling right that facilitates the exercise of other rights and, in some instances, contest decisions made by government particularly those which rely upon data or machine enhanced decision-making.

Digital government necessitates adapting existing practices to the digital environment to future proof the right to access information. In late September 2020 to mark Right to Know Week 2020 the Information Commissioner will release guidance to agencies and citizens to ensure the preservation and promotion of the right to access information. The guidance focuses on automated decision-making and digital government. In summary agencies are advised to ask three fundamental questions when developing digital solutions:

- Who holds the information?
- In what form is it held?
- How will access be provided?

As these systems are adopted by governments, citizens will increasingly be subject to actions and decisions taken by, or with the assistance of, automated decision-making systems. To fully exercise their rights, it is important that individuals can access information about how a decision is made and what information was used to reach that decision. Guidance, to be issued by the Information Commissioner advises citizens to ask four key questions:

- Who holds the information: for example, is it a government agency, taskforce or a contractor who is providing government services?

- In what form is the information held: for example, is it in a data set; is it a source code; an algorithm?
- How will access be provided: for example, in a data set; in a document that describes the source code or a test suite of data?
- Will I need assistance in interpreting the information; for example, are there other documents that I will need to access to understand or interpret the information?

The resources developed by the IPC support the commitment to better services through digital government and contribute to the commitment to develop the capabilities of the NSW Public Sector that is responsive to digital government and respectful of citizens' rights.

Conclusion

With the growth of digital service delivery by government and the increased use of technologies such as artificial intelligence and automated decision making, strong and effective cyber security measures are essential to maintaining public trust in the integrity of information held by government. The Information Commissioner and Privacy Commissioner support the implementation of robust cyber security measures to ensure the security of information held by NSW government agencies.

The Information Commissioner and the Privacy Commissioner recognise that the development and implementation of new technologies and modes of service delivery have the capacity to enhance the citizen's experience of government. At the same time, these developments introduce potential new risks of harm. Maintaining the trust and confidence of citizens that their rights will be protected will contribute to the success of digital government.

As an independent regulator with expertise in information access and management, data governance and privacy, the Commissioners welcome the opportunity to make a submission to the Committee.

Yours sincerely

Elizabeth Tydd
CEO, Information and Privacy Commission NSW
Information Commissioner
NSW Open Data Advocate

Samantha Gavel
Privacy Commissioner