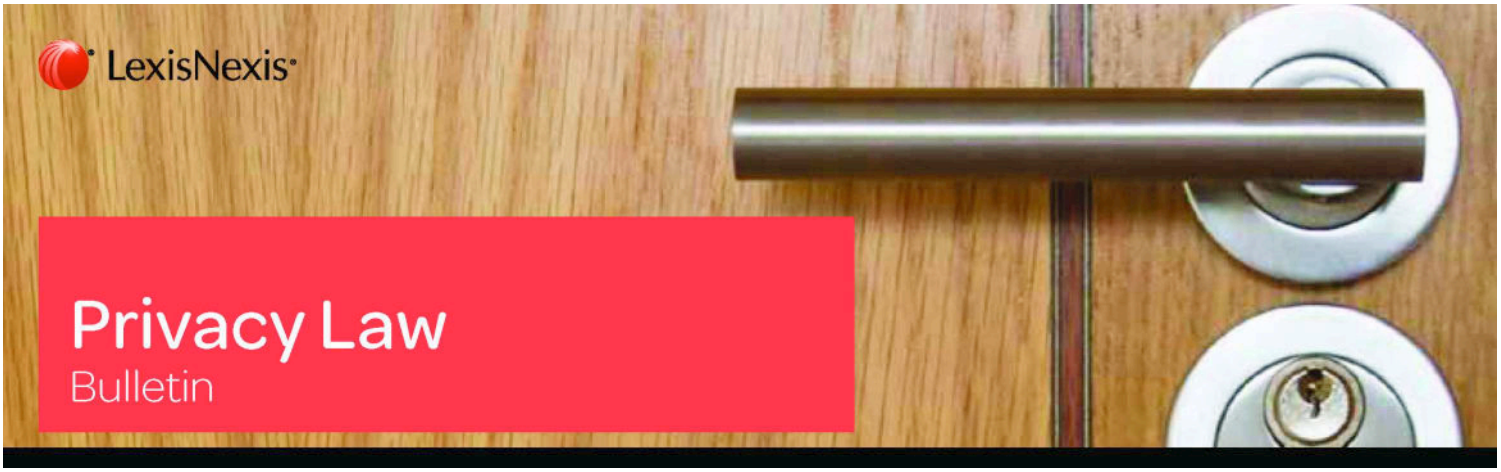

Privacy Law Bulletin

2020 . Vol 17 No 4

Contents

Information contained in this newsletter is current as at July 2020

LexisNexis Butterworths

Privacy Law
Bulletin

How to notify a data breach in 30 days

***Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** PIPER ALDERMAN*

COVID-19 has seen an increase in cyber attacks. This article outlines how to respond to a cyber attack leading to a data breach. It discusses:

- which regulatory bodies to report to
- the requisite information that must and should be provided to affected customers when advising them of the breach and
- remediation and penalties

Eligible data breach

An eligible data breach will occur if there is:

- unauthorised access to
- unauthorised disclosure of or
- likelihood of unauthorised access or disclosure of,

personal information, where a reasonable person would conclude that the disclosure would likely result in serious harm to any of the individuals and there is an inability to prevent the likely risk of serious harm with remedial action.[1]

When to notify

If an entity suffers or is suspected to have suffered an eligible data breach, it must provide a report to the Office of the Australian Information Commissioner (OAIC) and the affected individuals. Reporting should occur as soon as possible to minimise the risk of harm. In any event, the investigation of the incident and subsequent reporting should occur within 30 days of the incident.

Entities should take care to notify any affected individuals as soon as reasonably possible to alert them of the data breach and how they may have been affected.

The breach may need to be reported to other bodies. These include:

- Australian Federal Police through the Australian Cyber Security Centre (ACSC)
- the entity's Board of Directors and/or shareholders
- relevant government bodies in circumstances where government identifiers have been compromised eg tax office if the breach involves a disclosure of tax file numbers
- Australian Securities and Investments Commission (ASIC) through the Australian financial services licence (AFSL) breach reporting regime (and soon to be Australian credit licence (ACL) breach reporting regime) or
- the ACL Annual Compliance Certificate and Australian Competition and Consumer Commission (ACCC) Scamwatch

The most appropriate bodies to report to would depend on the circumstances of the breach. Affected entities should also notify their relevant insurance providers of the data breach.

A data breach does not directly raise liability with the Privacy Commissioner. However, entities may be liable if the Commissioner considers that there is a serious or repeated failure to comply with its obligations under the Privacy Act. This would arise in instances where an entity has breached the Australian Privacy Principles (APPs) or fails to meet the reporting or notification obligations under Pt IIIC of the Privacy Act, so it is imperative that the entity ensures that it complies with these obligations.

OAIC reporting

There are two stages involved in reporting to OAIC.

The first stage includes preparing a statement to provide to the Information Commissioner and the second is to take the reasonable steps and notify individuals and companies who have been affected by the breach. A report should be made as soon as practicable after becoming aware of the breach. Reporting entities should also provide a copy of the statement sent to affected individuals to the Information Commissioner.

The eligible data breach statement to the OAIC needs to include:

- the entity's name and contact details[2]
- a description of the eligible data breach — this needs to include information such as:[3]
  - — the date (or date range) of the unauthorised disclosure or breach
  - — the date the data breach was detected
  - — the circumstances of the data breach

  - — who has obtained or is likely to have obtained access to the information — the OAIC would be satisfied that the entity has to date been able to identify that the attacker appears to be an external third party and
  - — relevant information about the steps the entity has taken to contain or remediate (if possible) the breach
- the kind or kinds of information involved in the eligible data breach[4] and
- what steps the entity recommends that individuals take in response to the eligible data breach[5]

Customer notification and alerts

The manner of notifying affected individuals will depend on the nature of the breach and will generally be in the manner that customers usually use to contact individuals. Communications must also be secure and reasonably allow individuals to continue to protect their privacy.

Affected individuals should also be notified of the data breach which can be done through the issuing of a statement. This must include:

- the identity and contact details of the entity
- a description of the eligible data breach
- the kind or kinds of information involved in the eligible data breach and
- what steps the entity recommends that individuals take in response to the eligible data breach[6]

If an entity's company name is different to its business or trading name, the OAIC has recommended that they use the name which is most familiar to individuals and to ensure the proper contact details have been included.

In their statement to individuals, the OAIC recommends entities include the requisite information concerning the data breach so that affected individuals are able to properly assess the consequences of the data breach for themselves and take proactive and protective actions in response. Additional specific information regarding the eligible data breach that should also be notified includes:

- the date, or date range, of the unauthorised access or disclosure
- the date the entity detected the data breach
- the circumstances of the data breach (such as any known causes for the unauthorised access or disclosure)
- who has obtained or is likely to have obtained access to the information and
- relevant information about the steps the entity has taken to contain or remediate the breach

Depending on the severity of the breach, entities should also consider providing customers with additional information. Entities may wish to direct customers to where they may be able to locate the latest updates and FAQs about the breach or direct customers to update their password and security checks. Customers should also be provided with external privacy and security guidance on the OAIC's website and the relevant references. This may be an ACSC reference number if a police report has been made. Entities could also identify any remediation services available such as IDCARE support services or credit report monitoring by credit bureaus.

Remediation

Consequently, if the data breach is the result of a malicious attack, there is potential that the attacker can hold onto the stolen information for any period. Therefore, there is a need to be vigilant and maintain ongoing monitoring services to protect individuals' information.

Appropriate steps to take if an individual's identification or financial information has been accessed or stolen include:

- engaging a credit reporting body and service that will notify individuals if there is any activity on their credit report
- telling individuals to notify their authorised deposit-taking institution (ADI) so they can cancel their bank cards, obtain new ones and monitor transactions on their account
- recommending IDCARE services to assist with personalised case management in addressing any specific identity or personal information concerns affected individuals may have and to assist in navigating any additional response measures affected individuals may wish to take and
- provide dark web monitoring services to be notified if the stolen data is being sold online

Penalties

The legal consequences for breaches of the Privacy Act may include a public investigation resulting in civil penalties of up to 10,000 penalty units — $2.1 million at the time of writing.

The potential for reputational damage can be even more harmful. The inevitable public relation issues nightmare following a data breach can cause considerable financial damage and has the potential to impact future revenues.

Future litigation concerns

Individuals may have a right to sue for loss suffered as a result of a data breach under Australian law. They may bring a claim in contract if the contract includes provisions regarding liability for loss or damage as a result of negligence or a data breach, or a claim in tort for breach of privacy. Any claim regarding negligence would likely be unsuccessful if it is demonstrated that reasonable steps were taken to prevent the breach and mitigate loss suffered.

Directors are subject to a corporate officer's duty of care, skill and diligence under s 180 of the Corporations Act 2001 (Cth). Directors and officers may be found to have breached this duty if it is found they did not have effective procedures in place to comply with data protection obligations and the breach notification regime.

These potential liabilities emphasise the need to ensure that entities carefully manage the steps it has taken to investigate the email scam, mitigate damage to affected email recipients and comply with its obligations under the Privacy Act.

In conclusion, when a notifiable data breach has occurred, entities should take the proper cautionary steps to identify the harm and notify the requisite bodies about it. As there are reporting guidelines provided by the OAIC, it is important that entities comply with them and clearly identify the information requested.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au
www.andreabeatty.com.au

Chelsea Payne
Lawyer
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Chloe Kim
Law Graduate
Piper Alderman
ckim@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. Privacy Act 1988 (Cth), s 26WA.
2. Above, s 26WK(3)(a).
3. Above n 1, s 26WK(3)(b).
4. Above n 1, s 26WK(3)(c).
5. Above n 1, s 26WK(3)(d).
6. Above n 1, s 26WK(3)(a).

Digital signatures in the COVID-19 world

Charles Harrison *and* ***Martin Slattery*** *CARROLL & O'DEA LAWYERS*

Introduction

Given the COVID-19 world in which we now all operate, we are likely to see an increased use of digital signatures in the legal and commercial spheres going forward. Whilst courts generally consider that digital and electronic signatures are "a fact of modern commercial life",[1] it is important for businesses and individuals to consider how their private data and information is stored, processed, maintain, accessed and secured.

Key points/how does it affect you

What are digital signatures?

Digital and electronic signatures have been used in the commercial and legal industries since at least 2000. At the Federal level, the use of digital and electronic signatures is governed by the Electronic Transactions Act 1999 (Cth) (Commonwealth ETA). There are similar statutes in each state and territory.[2]

Pursuant to s 10 of the Commonwealth ETA, electronic and digital signatures will have the same effect as written signatures where the requirements of "identity",[3] "reliability",[4] and "consent"[5] have been satisfied.

Although there is some debate over exact definitions:

- A "wet signature" refers to an individual physically marking a document (ie with a pen).
- An "electronic signature" refers to the acknowledgement or adoption of an electronic message, transaction or document (ie an "electronic version" of someone's signatures which is placed onto a document, a typed name on an electronic form or document, a scribbled name on a device following a delivery).
- A "digital signature" uses "cryptographic authentication technology" which is an encryption sitting underneath the signature and provides for the tracking of each step of the execution/signature process and can assist parties (and a court) in determining who actually signed the document and when they purportedly signed it. Programs such as Adobe EchoSign and DocuSign are now commonly used by businesses and individuals to facilitate digital signatures.

Whilst in times gone by, there would have been a crowded boardroom with individuals — dressed in nice suits — attending to the signing of voluminous amounts of paper (within nicely laminated folders), this is increasingly becoming an antiquated form of operating. Obvious benefits of digital signatures are that it makes commercial dealings more efficient, quick and cost-effective. And it saves paper and improves sustainability.

What are the privacy considerations?

Digital signatures necessarily involve the uploading and exchange of documentation in a cloud platform. A question arises as to commercial confidentiality when documents are uploaded to cloud platforms. Companies who provide these services purport that when documents are uploaded to their platform, the substantive content of the document, agreement, contract or the like is encrypted; meaning they have no control over, or access to, the specific contents of the documents.

In engaging an external service provider to store documents and information in the cloud, individuals and companies must be satisfied that the cloud service provider can adequately protect the security of documents and other data. They should also be satisfied that documents uploaded to the platform are protected from unauthorised amendments, which is a particular risk with an increase in cybercrime and hacking, both nationally and globally.

A key consideration is where the cloud server (which hosts the relevant contents and data) is located. Where the server is hosted overseas, it will generally be subject to both its local laws regarding data protection and the laws of the nation hosting the server. Foreign government agencies can — legally — have more extensive powers to access information. Realistically, is it likely that companies, let alone individuals, are going to examine the small print of where the data is going to be stored? Maybe ... but maybe not and the risk of not doing this is that it could result in a material breach of private information.

What protections exist in Australia?

The Privacy Act 1988 (Cth) governs and regulates how relevant businesses handle personal information. Personal information is defined as any information or

opinion about an individual who is "reasonably identifiable". Businesses subject to the Privacy Act (ie a business with an annual turnover of $3 million) are subject to the obligations set out in the Australian Privacy Principles (APP).

The obligations can be summarised as follows:[6]

- The privacy policies of cloud providers must notify customers as to what personal information will be collected and state the intended disclosure arrangements of that personal information, including whether it will be placed in any international data storage locations.
- Cloud servers can only disclose personal information internationally if the overseas recipient does not breach the APPs.
- Cloud servers must give customers their personal information upon request.
- Cloud providers must take reasonable steps to secure personal information from misuse, interference or loss and from unauthorised access, modification or disclosure, including security breaches that occur internationally.
- Cloud providers must take reasonable steps to delete or de-identify personal information that is no longer needed for the purpose for which it was originally stored.

There will also, in appropriate scenarios, be remedies available under the Australian Consumer Law as it provides customers with protections including, but not limited to, those involving false and misleading conduct, unfair contractual terms and unconscionable conduct.

APP 8 and APP 11

APP 8 states that a relevant entity (such as a cloud server) which discloses personal information about an individual to an overseas recipient must take "such steps as are reasonable in the circumstances" to ensure that it complies with the APPs generally. In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under s 16C of the Privacy Act, to have been done, or engaged in, by the APP entity and to be a breach of the APPs.

APP 11 states that if a relevant entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss; and from unauthorised access, modification or disclosure. APP 11 further holds that such personal information is destroyed or de-identified once the entity no longer requires the information.

Importantly, the Federal Court can impose civil penalties of up to $2,100,000 per breach for each serious and/or repeated interference with an individual's privacy.[7] Therefore, there is an incentive for cloud servers that facilitate exchange of documents via digital signatures to comply with the Privacy Act and the APPs.

Best practice

Best practice for Australian cloud servers will be to ensure that they operate in accordance with the Privacy Act and other global privacy regimes and standards, such as the European General Data Protection Regime. Such practices will involve allowing customers to submit requests regarding their personal data, customers to determine their account retention policies, allowing customers to choose where their data will be located, and having privacy policies which are easily accessible and understandable (to the non-Bill Gates' of the world).

Conclusion

As technology in this area becomes increasingly sophisticated and more widely and regularly used, it is likely that breaches of the Privacy Act will rise and result in financial penalties. It is important for both servers which facilitate the exchange of documents using digital signatures and for companies/individuals who utilise such services to be aware of their rights and obligations when it comes to privacy and, in particular, the storage and maintenance of personal and/or important data.

Charles Harrison
Associate
Carroll & O'Dea Lawyers
charrison@codea.com.au
www.codea.com.au

Martin Slattery
Partner
Carroll & O'Dea Lawyers
mslattery@codea.com.au
www.codea.com.au

Footnotes

1. *Stuart v Hishon* [2013] NSWSC 766; BC201303109 at [34].
2. Including the Electronic Transactions (Victoria) Act 2000 (Vic), the Electronic Transactions Act 2000 (NSW), the Electronic Transactions Act 2000 (Tas), the Electronic Communications Act 2000 (SA) and the Electronic Transactions Act 2011 (WA).
3. Electronic Transactions Act 1999 (Cth), s 10(1)(a).
4. Above n 3, s 10(1)(b).
5. Above n 3, s 10(1)(c).

6. Australian Government Department of Communications *Cloud Computing and Privacy: Consumer Factsheet* (2014) www.communications.gov.au/sites/default/files/2014-112101-CLOUD-Consumer-factsheet.pdf?acsf_files_redirect.

7. Privacy Act 1988 (Cth), ss 80W and 13G.

Privacy Law
Bulletin

Current status of China's cybersecurity — data protection laws

Dr Robert Walters *VICTORIA UNIVERSITY*

China has emerged as an international leader in many areas of technology.[1] The cybersecurity laws that were recently implemented have evolved to not only serve the sovereign needs of the state but also provide a level of protection to its citizens' personal data over the internet. It would be incorrect to think that China does not consider privacy as a broader concept or right that requires protection. This article will discuss the current status of China's data protection and cyber laws that, in part, provide a level of privacy protection. It will focus on the important principles of the law, the concept of consent and the definition of personal data-information.

Introduction

According to Li-ming Wang,[2] there have been four stages of development of privacy in China including:

1) protection by analogy[3]
2) personality interest protection[4]
3) protection by tort law[5] and
4) a separate human right under Art 110 of the General Provisions of the Civil Law that was enacted in 2017

Over the past 5 years there has been a significant transformation in data protection-cybersecurity law in China. In March 2018, the National Information Security Standardisation Technical Committee of China (TC260) issued a national standard, the Personal Information Security Specification which covers the collection, storage, use, sharing, transfer and disclosure of personal information.[6] Wei Sheng is of the view that the Personal Information Security Specification[7] has many similarities to that of the European Union General Data Protection Regulation (GDPR).[8] The Constitution of the People's Republic of China (PRC) provides for the "personal dignity" and "residences" of citizens are inviolable and that citizens' "freedom and privacy of correspondence" are protected by law.[9] The General Principles of Civil Law further provides that:

> All citizens and legal persons are entitled to the right to reputation. The personal dignity of citizens is protected by law. The use of insults, defamatory statements and other means to damage the reputation of citizens and legal persons is prohibited.[10]

The Cybersecurity Law of the PRC (Cybersecurity Law),[11] provides the basis for data protection. On 1 October 2019, China's Regulations on Network Protection of Children's Personal Information came into effect.[12] Article 1 of the Cybersecurity Law provides that this law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organisations, and promoting the sound development of economic and social information.[13]

Article 22 provides that network products and services shall comply with the compulsory requirements of relevant national standards. Providers of network products and services shall not install malware. When a provider discovers any risk such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures, inform users in a timely manner and report it to the competent department in accordance with relevant provisions. Providers of network products and services shall continuously provide security maintenance for their products and services, and shall not terminate the provision of security maintenance within the stipulated period or the period agreed upon by the parties.

Principles of personal information security

Rather than the Cybersecurity Law highlighting the general principles of personal information protection, this has been left to the Information Security Technology Personal Information Security Specification (ISTPISS).[14] The ISTPISS places considerable obligations on personal information controllers to implement the principles and is enforceable. The ISTPISS requires that the management of personal information be undertaken commensurable to powers and responsibilities that minimise the damage to the lawful rights and interests of the personal information subject.

The Cybersecurity Law arguably takes a greater focus on securing the infrastructure through formulating and continuously improving cybersecurity strategies,

policies and procedures for key sectors.[15] That is:

- Article 5 reinforces this point whereby the state is required to monitor and prevent cybersecurity risks and threats arising both within and without the mainland territory of the PRC.
- Article 6 is an important expression of the sovereign needs of the state and reinforces its current governance arrangements. It enables the state to promote and advocate the notion of cybersecurity more broadly in a sincere, honest, healthy and civilised way to require the conduct of individuals to be undertaken according to the core socialist values of the state.
- To protect the state, Art 7 enables international exchange and cooperation in areas of cyberspace governance, research and development of network technologies, formulation of standards, and follow up crackdown of cybercrime and illegality. Article 7 goes on to promote an environment of peaceful, secure, open and cooperative cyberspace by establishing a multilateral, democratic and transparent internet governance system.
- Article 9 requires that network operators carrying out business and service activities not only comply with the law but also abide by commercial ethics, be honest and credible, perform obligations to protect cybersecurity, accept supervision from the government and public, and bear social responsibility.
- Article 10 places a level of responsibility on those individuals and entities constructing and operating these networks to ensure they are developed according to national standards.

They are required to adopt technical measures to safeguard cybersecurity while ensuring operational stability, and as efficiently as possible, respond to cybersecurity incidents.

Definition of personal data

China's Cybersecurity Law does not define personal data or personal data-information or sensitive personal data-information. However, such a definition can be found in the ISTPISS for both personal and sensitive personal information. Firstly, personal information constitutes all information whether recorded by electronic or other means. It also means that that information can be used alone or combined with other information and can identify a natural person. Personal information also extends to that information that reflects the activities of the natural person. A person able to be identified from their activities is a unique feature of the framework, and is something that is not explicitly stated in developing countries' laws. Nonetheless, personal information includes name, date of birth, identity card numbers, biometrics, addresses, telecommunication contact methods, communication records and content, account passwords, property, credit, location data, accommodation, and health, physiological and transaction information. Sensitive personal information includes information that once leaked, illegally provided or abused can threaten the personal and property security of the individual. It also extends to that information that can cause personal reputational, physical or mental health damage, or discriminate against the individual. Similar to general personal information, sensitive information includes identity card numbers, biometrics, addresses, telecommunication contact methods, communication records and content, account passwords, property, credit, location data, accommodation, and health, physiological and transaction information. It also includes all personal information pertaining to children under the age of 14,[16] which has been afforded extra protection in 2019.

Protections

While there is no formal recognition of the Right to Be Forgotten, the ISTPISS extends the rights of citizens to seek that their personal information is managed to rectify and correct an error or if that information is incomplete, the controller is to modify the information.[17] Moreover, Art 7.6 allows a data subject to request of a controller that their personal information be deleted. However, the ability for personal information to be deleted can only be achieved when a controller has violated the laws in relation to the collection of that information, or the agreement for the collection of that information has been violated. This also extends to any agreement for the transfer of the personal information to third parties and disclosure of that information. Any transfer to a third party is to cease as soon as possible upon receipt of a request by a data subject for the deletion of their personal data. The disclosure of personal information is to also cease as soon as the data subject has requested that it be deleted.

Consent

Consent is neither defined or described in terms of how and what it might constitute. Arguably, the fluid nature of the term has been developed to meet China's sovereign needs, with such a large population when compared with many other countries in the world. The ISTPISS describes how the concept of consent operates in relation to personal information. In other words, prior to the collection of personal information authorised consent is to be obtained by the controller.[18] While it is not clear as to what authorised consent means, it applies to the purpose, manner, frequency of collection along

with the storage location and period to which the information will be stored (the controller's data security capabilities, information related to sharing, transfer and public disclosure). On the other hand, when personal information is collected indirectly there is a requirement on the provider of that information to inform the recipient of the information source and ensure its legitimacy has been confirmed. Again, the processor of the personal information that has been collected indirectly is to understand the authorised consent, including the purpose, sharing, transfer and public disclosure.

However, where an organisation needs to process the personal information for its own business needs, which are beyond the scope of the initial authorised consent, the organisation will need to obtain explicit consent from the data subject. Nevertheless, there are exceptions to the above, and the controller responsible for handling personal data is not required to obtain authorised consent for the collection and use of that information when it directly relates to national security, national defence, public safety, public health and interest.[19] It also applies to criminal investigations, prosecution, trial and judgment of enforcement. Further exemptions apply when there is a need for safeguarding major lawful rights and interests pertaining to property of the data subject or other persons, and moreover, when it is difficult to obtain the consent from the data subject. The exemptions also extend to when the data subject voluntarily allowed the collection of their personal information by the general public. This would likely arise when individuals upload their personal information to apps and websites that are generally available to the broader public. When the personal information has been made public for example, through news reports and open government information, authorised consent is also not required. It also pertains to when it is necessary to sign and perform a contract that has been agreed and approved with a data subject, and to maintain the safe, stable operation of products and services.

On the backdrop of the above exemption(s), the requirement for a controller to obtain explicit consent for the collection of sensitive personal data extends to when a data subject has provided the information freely, and it is specific, clear and unequivocal.[20] Additionally, there are further requirements whereby a controller collects personal sensitive information. Thus, prior to the collection of this information, whether voluntarily or automatically, the controller is to inform the data subject of the core function of the provided products or services and the sensitive information that will be collected. The controller is also required to disclose the impacts which may occur if the data subject refuses to provide it or refuses to provide consent. Note that below there are different requirements for consent for children who are 14 years old or younger. Controllers are encouraged to provide options to the data subject, whereby they are to allow the subject to choose whether the provisions or automatic collection of sensitive data should be allowed. In practice, it would be interesting to better understand how this operates. However, where the products or services provide additional functions and sensitive personal information is collected, the data subject would need to be fully informed as to why that information is being collected. Importantly, where the data subject rejects the collection of that sensitive data, effectively the function of collection is to cease.[21] However, any request to cease the collection of data should not impede the business operations of the organisation. For instance, this would be important information for a hospital, yet a local garage that services one's car might not require sensitive personal information to be collected and used.

Children

The year 2019 marked, in our view, a significant turning point in China's approach to protecting personal data over the internet. They established a very important legal initiative to provide further protection for children online. While, in large part, the new controls do resemble the developments of the EU, China subtly digressed from the European equivalent. On 22 August 2019, the Cyberspace Administration of China (CAC) released a new data privacy regulation related to children, the Provisions on Cyber Protection of Personal Information of Children (儿童个人信息网络保护规定) (PCPPIC).[22] The regulation came into effect on 1 October 2019 and applied within the PRC. The PCPPIC's purpose is to protect the security of children's personal information and promote the healthy growth of children in the PRC. However, the PCPPIC is limited to minors under the age of 14 but leaves a regulatory gap for minors aged 14 or above.[23] In particular, this could also give rise to issues such as what rights minors will have in relation to their personal information which has already been collected when they reach the age of 14 and whether they should be treated as adults under data protection laws at that time. Furthermore, the 29 Articles sets forth high-level requirements for the collection, storage, use, transfer and disclosure of the personal information of children within PRC territory.

Moreover, in our view, one of the most important inclusion China has introduced is the expansion on the concept of consent for children 14 years old and younger. That is, the new laws require data controllers the personal information (data) of children as sensitive information. They must obtain express consent from the child's guardian(s) for the processing of personal information. The special protection measures applicable to sensitive personal information under the ISTPISS will

also apply to children's personal information. The law further provides that these required measures include separate consent for each function of a service or product, encryption of data for storage and transmission, request-based internal access authorisation, prior notification and express consent before data sharing or transferring. The model privacy policy attached to the ISTPISS also includes a section on processing of children's personal information.[24]

There are six key areas where consent will be required from a guardian, including;

- purpose, scope, method, and term of collection, storage, use, transfer and disclosure of information
- the storage location and treatment of information after the agreed term expires
- security measures to keep information protected
- consequences for parents or guardians who refuse to provide consent
- platform where parents or guardians can report violations or file complaints with the network operator in regard to mishandling children's personal information
- consent will be viewed as necessary when methods for the revision and deletion of children's personal information, or a substantial change by network operators are required to re-obtain parental or guardian consent[25]

The PCPPIC establishes a framework that requires parental/guardian consent and network operator responsibilities to protect children's data privacy. However, one of the fundamental differences are the age limitations. In the EU, the GDPR has an age limit of 16,[26] whereas China has 14. However, in accordance with Art 8 of the GDPR, member states of the EU can regulate to the age of 13 years.

Proposed 2020 law reform

In 2020, it has been reported that China will embark on implementing more specific data protection laws. It is proposed that China will implement two separate laws: 1) the Personal Data Protection Law and 2) Data Security Law in 2020, which are a matter of priority.[27]

Qiheng Chen[28] believes that the draft adopted a contractual approach to transferring data from domestic network operators to foreign data receivers. This approach draws from the EU GDPR's binding corporate rules that allow multinational companies to transfer data internationally between their subsidiaries. Another development is a provision to allow the termination of cross-border data transfers if the contract cannot be implemented due to changes to the legal environment of the country where the recipient is located. This clause can be interpreted as a response to extraterritorial data laws such as the United States' Clarifying Lawful Overseas Use of Data (CLOUD) Act.[29] The draft cemented the separate treatment of personal information and important data. The latter refers to information that, if leaked, may infringe on national security. The new draft focused solely on the outbound transfer of personal information which hinted at a forthcoming twin draft for important data.[30] In addition, consent is likely to be diluted. Currently, no outbound transfer would be allowed without consent by the personal information subject. The proposal is likely to result in consent being needed only for the onward transfer of sensitive personal information — a small subset of personal information — to third parties.[31] However, these new proposals require further vigilance until China releases the final versions that will be implemented.

Conclusion

The concept of privacy in China is complex. They have, to date, taken a greater focus on establishing strong laws around protecting the systems, platforms and infrastructures. China's approach is better understood as a kind of policy guideline or regulation and that government authorities are likely to refer to the specification when conducting various reviews.[32] Finally, further vigilance will be required by practitioners once China releases their updated laws.

Dr Robert Walters
Lecturer, Victoria University
Adjunct Professor, European Faculty of Law, Slovenia, Europe
robert.walters2@live.vu.edu.au

Footnotes

1. Thanks to Associate Professor Jeanne Huang, University of Sydney and Professor Leon Trakman, University New South Wales for looking over this article which forms a chapter in a forthcoming book by Robert Walters and Marko Novak on Cyber Security, Artificial Intelligence and Data Protection Law. The book discusses the intersection of these three areas of law and compares China, Hong Kong, Macau, Taiwan, South Korea, Philippines, Laos, Vietnam, United States and Canada's data protection laws.
2. Li-ming Wang, "Privacy Protection in China: Paths, Characteristics and Issues" (The International Conference of Data Protection and Privacy Commissioners, Hong Kong, September 2017), www.privacyconference2017.org/eng/files/programme_booklet.pdf.
3. Above.

4. Above n 2. Article 1 of the Interpretation of the Supreme People's Court on Problems Regarding the Ascertainment of Compensation Liability Compensation for Emotional Damages in Civil Torts.
5. Above n 2. Law of Tort enacted in 2009.
6. Wei Sheng, One year after GDPR, China strengthens personal data regulations, welcoming dedicated law, 19 June 2019, https://technode.com/2019/06/19/china-data-protections-law/.
7. Mingli Shi, Samm Sacks, Qiheng Chen and Graham Webster, Translation: China's Personal Information Security Specification, 8 February 2019, www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/; Information Security Technology Personal Information Security Specification Chinese version: www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf.
8. Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.
9. Cybersecurity Law of the People's Republic of China, Order No 53, Arts 38–40, http://en.pkulaw.cn/display.aspx?cgid=4dce14765f4265f1bdfb&lib=law.
10. Above n 9, Art 101.
11. Above n 9.
12. Sara Xia, China's New Child Privacy Protection Rules, 22 September 2019, www.chinalawblog.com/2019/09/chinas-new-child-privacy-protection-rules.html; Hunton Andrews Kurth LLP, China Issues Provisions on Cyber Protection of Children's Personal Information, 7 October 2019, www.huntonprivacyblog.com/2019/10/07/china-issues-provisions-on-cyber-protection-of-childrens-personal-information/.
13. Above n 9.
14. Above n 7.
15. Above n 9, Art 4.
16. Above n 7, Arts 3.1–3.2. Xia, above n 12; Hunton Andrews Kurth LLP, above n 12.
17. Above n 7, Art 7.5.
18. Above n 7, Arts 5.3–5.4.
19. Above.
20. Above n 7, Art 5.5
21. Above.
22. Karen Ip, Nanda Lau and James Gong, China Investments E-Bulletin: China's First Regulation On Children's Online Privacy, Herbert Smith Freehills, 16 September 2019, https://sites-herbertsmithfreehills.vuturevx.com/95/20753/september-2019/china-s-first-regulation-on-children-s-online-privacy.asp?sid=56d3bb39-faab-43a3-967a-6cbeb683e586&utm_source=Mondaq&utm_medium=syndication&utm_campaign=inter-article-link.
23. Above.
24. Above n 22.
25. Above n 22.
26. Above n 8, Art 8.
27. Scott Theil, Carolyn Bigg and Kenny Tam, China: Privacy, security and content regulation to increase in 2020, 14 January 2020, https://blogs.dlapiper.com/privacymatters/china-privacy-security-and-content-regulation-to-increase-in-2020/.
28. Q Chen "China's New Data Protection Scheme: China has released a draft regulation fleshing out its cybersecurity law" *The Diplomat* 2 July 2019, https://thediplomat.com/2019/07/chinas-new-data-protection-scheme/.
29. Above.
30. Above n 28.
31. Above n 28.
32. Samm Sacks, China's Emerging Data Privacy System and GDPR, 9 March 2018, www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

Privacy Law
Bulletin

The bottomless abyss of data in a technological and computerised world: The privacy of Australians' data and the Internet of Things

Murray Thornhill, Fintan Daniel Roberts *and* ***Kai Yuin Yeo*** *HHG LEGAL GROUP*

Introduction

In an increasingly technological and computerised world, constantly shifting privacy challenges have become commonplace. In the news recently, for example, we have seen how a significant breach of the data stored by Optus resulted in the data of 50,000 Australians being exposed.

Two recent developments have been in the expanding Internet of Things (IoT) and its interrelation with cloud computing. The interrelation of these two systems provides a vast array of benefits for improving the way in which we carry out work and organise our personal lives. However, while these systems may make our lives easier, they also pose significant privacy concerns.

What is the Internet of Things and cloud computing?

The IoT refers to "an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world".[1] These devices generate huge amounts of data based on usage, for example the number of times the doors of a smart refrigerator are opened or when a user would normally set an alarm using a smart assistant. It is important to note that, currently, this IoT technology does not enable the storage or organisation of the data in the connected devices, meaning that this collected data must be stored elsewhere. On its own, the data collected as part of the IoT would not be entirely meaningful.

However, cloud computing complements the IoT by providing a central remote location for the storage and retrieval of data generated by the IoT. In other words, cloud computing is what enables IoT devices to work efficiently.[2] Using infrastructure provided by cloud service providers, organisations and individuals are able to store, transfer and receive the data generated from IoT devices from any place, anytime. This, however, does not occur in some mystical virtual data-receptacle. Rather, the reality is that any information uploaded still has to be stored in a physical data centre.

Coupled together, we have a system where data about how we live our everyday lives is being stored in a central storage location accessible by the collecting organisation. This process is so discrete that we are often not aware that our data is being collected continuously as we use those devices. These devices also often work in sync with other devices in the same "family", such as syncing between Google products and services, or between Samsung products and services. These smart devices would not be able to do so without generating data and using cloud computing to organise the data.

As we move towards "smart cities", "smart transport", "smart living" and so on, the privacy issues associated with this progress and the necessity of development of adequate privacy protections remain important considerations.

Breaches of privacy

With the number of smart appliances skyrocketing into the technological infinity and beyond, so too will the number of cloud services that assist with storing and facilitating the transmission of that data from location to location.

Putting aside cybersecurity concerns such as deliberate hacking into systems, the mere fact that our information is transmitted over the internet, stored and organised into meaningful data to enable personalised user experience of a range of devices is enough to warn of potential breaches of privacy.

Tech giants such as Google, Apple and Amazon have come under scrutiny for breaches of privacy in relation to data that their smart devices such as the Google Home Assistant and Amazon's Alexa have collected. For example in 2017 Google Home mini devices received significant media interest after they were found to be recording and transmitting information back to Google when the users were not intending them to.[3]

Your information may be stored and accessed by various organisations due to all of the inadvertent agreements to uses of data that you may not realise you have agreed to. In addition to this, the expansion of data

collection through the IoT is likely to also result in, for example:

- online profiling and exclusionary targeting
- exploitation of consumer vulnerabilities through online profiling
- price discrimination using accumulated data

Privacy protections in Australia — concerns and improvements for the future

Under the Privacy Act 1988 (Cth), there are certain Australian Privacy Principles (APP) which prescribe the manner in which certain entities deal with the collection and use of data. These entities under the Privacy Act are called APP entities which include any private and non-profit organisations with an annual turnover of more than $3 million and data companies. These APP principles govern the way organisations can collect, use and disclose information about individuals in Australia.

The intended effect of these APPs is to ensure that entities make available an up to date privacy policy which clearly spells out what information they collect and how they use your information. In particular, they must not collect your information unless it is reasonably necessary for the entity's functions. They must also notify you of the data they collect and your rights in relation to the data.

However whilst APP entities must comply with the APPs, compliance in practice is different for each entity.[4] The frequent use of terms such as "reasonable" and "reasonably" in the Privacy Act to qualify a test or obligation on APP entities gives them some leeway to implement the APPs in a way that suits their business model. Unfortunately for consumers this means that there is not much clarity on whether an APP entity's actions have breached the APPs. With the lack of significant penalties and direct right of action for consumers, entities may also be less motivated to consider how best to comply with the principles.

Consumer information captured under the Privacy Act

The Privacy Act defines two types of information: personal and sensitive information. Personal information is defined as:

> … information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.[5]

To qualify as personal information, there must be a certain degree of connection between the information and the individual, which demonstrates that the information is "about" the individual. For example, personal information can include employment details such as work address, salary and job title, or a person's private details such as home address, telephone number or bank account details. Sensitive information is further information specific to such things as racial origin or political opinions.

The Australian Competition and Consumer Commission (ACCC) had, in its final report into the digital platforms inquiry dated 26 July 2019 (ACCC Final Report),[6] recommended that the definition for personal information be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data and any other online identifiers that may be used to identify an individual. While these types of data individually may not identify an individual, they can by correlation be used by Google or Facebook to identify data about an individual.[7]

This recommendation was made following various stakeholder submissions about the uncertainty in scope of the current definition and whether much of the data being collected would fall within the parameters of the Privacy Act's provisions. It was the general consensus from stakeholders that the definition should be made as broad as possible to encompass the continually expanding range of products and systems being introduced that capture data.

For example, the Internet of Things Alliance Australia submitted that sensing and actuating products such as the range of Google Home products have increased Google's ability to capture information from the home that "may, over time, through the use of data analytics, yield highly personal information such as home occupancy and a wide range of behaviours". It was further submitted that much of this collected data would not currently be considered personal information.[8]

Accessibility of dispute mechanisms and complaint procedures

Without effective dispute mechanisms and complaint procedures for Australians to remedy any actual or potential breaches of their privacy, the above discussions simply become academic.

Under the existing regulatory framework, the Privacy Act currently does not allow individual consumers to take any direct action against digital platforms or other organisations that are APP entities to seek compensation for mishandling personal or sensitive information therefore providing them with limited recourse. This means that consumers have to rely on other bodies to take action on their behalf, which due to resource constraints is unlikely unless a mass class action is unveiled.

What recourse individuals do have under the Privacy Act is constrained to making a complaint to the Office of the Australian Information Commissioner (OAIC) after

first complaining directly to the APP entity itself. Outcomes that can result from an OAIC complaint include being issued an apology, having a change made to the practices or procedures of the organisation complained of, or compensation for financial or non-financial loss. However, it should be kept in mind that as an organisation with limited resources, the OAIC have the discretion to decide which investigation to pursue and the lengths to which they are willing to go. Whilst the OAIC can investigate complaints for free, the investigation may take some time to complete due to conciliation requirements and the results may not always be ideal for complainants. For example, in the event that the OAIC does actually take legal action for a "very serious breach" by seeking a civil penalty, that civil penalty is not actually paid to the complainant.

It may be prudent for the legislature to create a direct right for individuals to bring actions and class actions under the Act against APP entities, as recommended by the ACCC,[9] particularly in light of the increasing number and types of IoT connected devices in the market. This right of action in the Federal or Federal Circuit Court would allow individuals to seek compensation for interferences with their privacy and overcome the current shortcomings with current dispute mechanisms. It will also further ensure that APP entities are held accountable and incentivise them to comply with the Privacy Act.

A path forward — the EU GDPR and industry self-regulation

Transparency of data collection and consumer understanding of exactly what personal and sensitive individual data is being held and stored by different organisations are core privacy issues. Much of this comes down to the ease in which consumers can enter into contracts to start using these various products and services, and the cloud of mystery which tends to overshadow digital activities. Contracts are, now more than ever, easily entered into through the exercise of everyday motor habits. For instance, when you tick a check-box to gain access to a service such as a phone application , or quickly agree to terms and conditions for the use of websites and other miscellaneous applications, or otherwise enter into user agreements for various software products.

As foreshadowed by the ACCC, many Australians:

- are not fully aware of their privacy rights and
- do not feel empowered to exercise those rights, particularly in dealings in respect of digital data

These concerns may be addressed by adopting some of the provisions from the General Data Protection Regulation (GDPR) and by implementing a comprehensive educative scheme.

GDPR

The GDPR contains a set of Articles created by the European Union (EU) to regulate data protection and privacy.[10] The requirements of the GDPR are far stricter than those contained under the Privacy Act, and were introduced as recently as May 2018.[11] The GDPR, despite being in operation for such a short period of time, has already facilitated a number of investigations into how data collectors are handling users' data and discharging their GDPR obligations. This is evidenced by the 21 GDPR investigations recently launched by the Data Protection Commission of Ireland into organisations including Facebook, WhatsApp and Apple.[12] It can further be seen by the fine imposed on Google by the French data protection authority (CNIL) for breaching the GDPR by combining user data across its services — fining Google for violating their obligations of transparency and requirement to have a legal basis for processing personal information under the "ads personalisation" setting.[13]

But what parts of the GDPR would we want to incorporate into our privacy regime? One significant difference between the two systems is the definition of personal information, which is contained in Art 4 of the GDPR. That definition is far broader than the current Privacy Act definition, including identifiers discussed above in the context of the ACCC's recommendations such as location data and online identifiers.

Another key difference is that there is no Australian equivalent of the Right to Erasure (right to be forgotten) contained in Art 17 of the GDPR. As the title indicates, this Article entitles individuals to the right to obligate data controllers to erase personal data concerning the individual without undue delay. The closest thing we have to this is APP 11.3 which requires APP entities to destroy or de-identify information when that information is no longer needed (subject to the interpretative hurdles discussed above).

A further asset of the GDPR is Art 20 which provides the right to data portability. Pursuant to this article, individuals have the right to receive the personal data concerning him or her, provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another controller without hindrance. The closest similarity we have is the Consumer Data Right rules under the Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) which allows users to request their data in a machine readable format and allows users to switch between service providers easily. However, the Consumer Data Right rules currently only apply to the banking sector and are thus limited in application.

Furthermore, under Art 15, individuals have a right of access to obtain from the controller confirmation as to whether personal data is being processed, and where that is the case, access to the personal data accompanied by such details as the purpose of processing, categories of data, recipients or categories of recipient to whom the data is disclosed, and so on.

Also of note is the requirement imposed under the GDPR for controllers to implement data protection at the very start of manufacturing devices.[14] This requires controllers to think about how to protect data collected through the proposed inventions or devices at the outset, rather than as an afterthought. Some examples of how this might be done include minimising the processing of personal data, pseudonymising personal data as soon as possible, ensuring transparency in respect of the functions and processing of personal data and enabling individuals to monitor the processing.[15] There is no Australian equivalent to this article in the GDPR.

The compellability of the GDPR scheme stems from the control which it gives to consumers to regulate the use of their own data, cutting through the cloud of mystery that generally overhangs the digital arena. With the IoT and the huge amount of data IoT devices collect, it would be of great benefit for Australian legislation to provide users with the right to request access to and deletion of their data.

Education

In conjunction with the above, we consider that it will be necessary for an educative scheme to be introduced from the government level down, informing consumers of their rights and avenues of redress. It is crucial that consumers become fully aware of their rights and the obligations of data collectors to adhere to them. Consumers need not necessarily need to assert those rights — so long as consumers become conscientious of what rights they do have, the circumstances in which they waive those rights (such as by entering into user agreements or by continued use), the use that can be made of their information (both legally and from a practical point of view) and the standards of privacy to which their information should be kept.

The ACCC considered that ideal, competitive data-driven markets competing for well-informed consumers on all dimensions of price and quality, including level of privacy protections are achievable when competition, data protection and privacy, and consumer protection are balanced. This is, by description, effective industry self-regulation. The first step to achieving that would be to combine the incorporation of the legislative recommendations discussed above with a comprehensive and accessible educative scheme for consumers. This will then create conscientious consumers and a competitive market in which APP entities will be self-driven to provide for and adhere to the best, most transparent and involved privacy standards.

Conclusion

IoT connected devices are the new trend and they are not going anywhere anytime soon. In the wake of the increasing influence of the IoT and the surge of consumer data being collected, we should prioritise the steps to establish better privacy protections as follows:

- redefining personal information under the Privacy Act to ensure that all data is captured
- creating a direct right of action for individuals
- adopting or taking inspiration from some of the GDPR provisions, specifically Arts 4, 15, 17, 20 and 25 and
- providing an educative scheme from the government level down addressing all of the above changes and informing consumers of what rights they have to retrieve, delete and otherwise access personal data, as well as to provide information about how they can keep APP entities accountable for potential breaches or non-compliance with requests for data retrieval and/or deletion.

Murray Thornhill
Director
HHG Legal Group
Murray.Thornhill@hhg.com.au
www.hhg.com.au

Fintan Daniel Roberts
Lawyer
HHG Legal Group
fintan.roberts@hhg.com.au
www.hhg.com.au

Kai Yuin Yeo
Lawyer
HHG Legal Group
KaiYuin.Yeo@hhg.com.au
www.hhg.com.au

Footnotes

1. Organisation for Economic Cooperation and Development *The Internet of Things: Seizing the Benefits and Addressing the Challenges* OECD Digital Economy Papers No 252 (2016) https://doi.org/10.1787/5jlwvzz8td0n-en p 8.

2. Kiran Gutha, Internet of Things (IOT) vs Cloud Computing, 14 December 2017 https://yourstory.com/mystory/61064782df-internet-of-things-io.
3. Andrew Martonik, Google to disable touch-activated listening on Home Mini following reports of constant recording, 11 October 2017, www.androidcentral.com/google-disable-touch-activated-listening-home-minis-following-always-listening-reports.
4. Fleur Prins, GDPR versus the Australian Privacy Act, 22 October 2018, www.epiuselabs.com/data-security/gdpr-vs-australian-privacy-act.
5. Privacy Act 1988 (Cth), s 6(1).
6. Australian Competition and Consumer Commission *Digital Platforms Inquiry Final Report* (26 July 2019).
7. Australian Privacy Foundation *Submission to the Australian Competition and Consumer Commission on the Digital Platforms Inquiry Preliminary Report* (22 February 2019) p 4.
8. Internet of Things Alliance, Submission to the Australian Competition and Consumer Commission on the *Digital Platforms Inquiry Preliminary Report* (15 February 2019) p 1.
9. Above n 6, p 24.
10. Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.
11. Matt Burgess, What is GDPR? The summary guide to GDPR compliance in the UK, 24 March 2020, www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.
12. Chris O'Brien, Irish data agency investigates GDPR violations by Facebook and others, 20 February 2020, https://venturebeat.com/2020/02/20/irish-data-agency-investigates-gdpr-violations-by-facebook-and-others/.
13. Above n 6, p 439.
14. Above n 10, Art 25.
15. Information Commissioner's Office, Data protection by design and default, May 2018, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.

For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047
Cite this issue as (2020) 17(4) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067