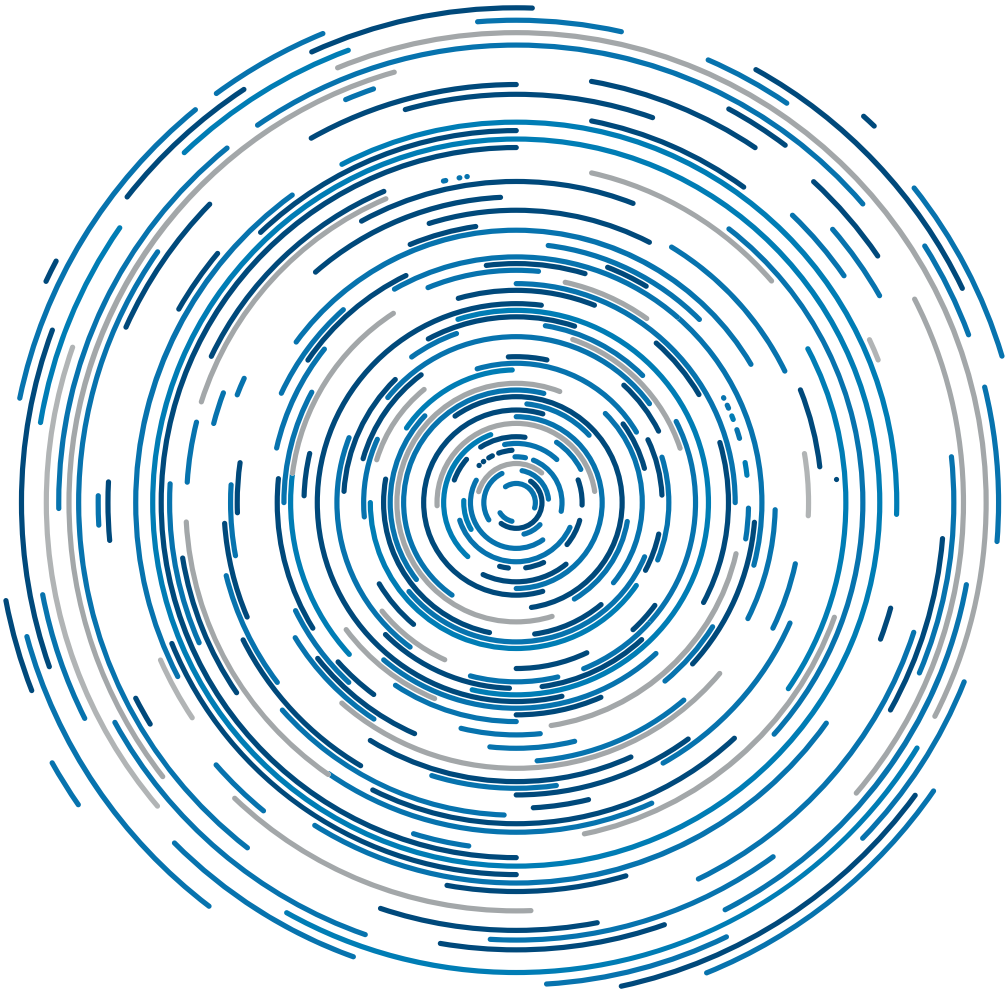
Deloitte.



Open banking

Privacy at the epicentre

June 2018

By giving customers control over their banking data, and the ability to share it with third parties, open banking will transform banking in Australia. It has also generated a renewed focus on privacy. Open banking will result in more entities accessing banking data, and banking data being transferred more often – increasing the possibility that data privacy is compromised.

These changes are occurring in an environment where individuals want confidence that their information is securely handled, where there has been a number of high profile privacy breaches, and where the global regulatory landscape is becoming increasingly strict.

The implementation of the General Data Protection Regulation (GDPR) in the European Union introduces a stricter privacy standard. GDPR will heavily influence privacy expectations and open banking in Australia. The Australian Senate has recently commented that it supports the drafting of GDPR-style laws in Australia.[1]

Notes

[1] See also https://www.itnews.com.au/news/senate-backs-greens-push-for-gdpr-style-data-laws-490702

As these two trends – open banking and an increased focus on privacy – collide, banks will need to rethink their traditional business model, and place customer privacy at the epicentre.

Until now, banks have largely captured the value of proprietary customer banking data – both personal and financial information – using it to inform their marketing and sales, as well as credit decisions and compliance activities such as financial crime risk management. The introduction of open banking based on the recommendations in the Farrell Report will give customers greater access to and control of their banking data.[2] Customers will have a right to access and share their banking data with third parties, so that they may obtain competitive or value added products and services.

Vital to a successful open banking scheme will be enhancing the customer experience, without compromising information privacy and security. Customers will only engage with open banking if they trust and understand it. To address this, the Farrell Report recommended the introduction of a national "Consumer Data Right" and proposed amendments to the Australian Privacy Act 1988 (Privacy Act).

The strategic approach: customers demand privacy and opportunity

Deloitte's Australian Privacy Index 2018 surveyed over 1000 consumers and identified that 41% are comfortable allowing a brand to transfer their personal information if they trust the brand and there are benefits in doing so.[3] This suggests that there is a willing cohort of customers ready to engage with open banking if they trust the brand of the data recipient.

However, it also means 59% of respondents are uncomfortable about transferring data – even if it is to a trusted brand. Organisations will need to actively inform clients about how open banking will benefit them, and demonstrate the value, to build this cohort's confidence in sharing data.

Deloitte's research indicates the importance of a balanced data ecosystem, where the exchange of customer data balances transparency, security, and the fair exchange of value.

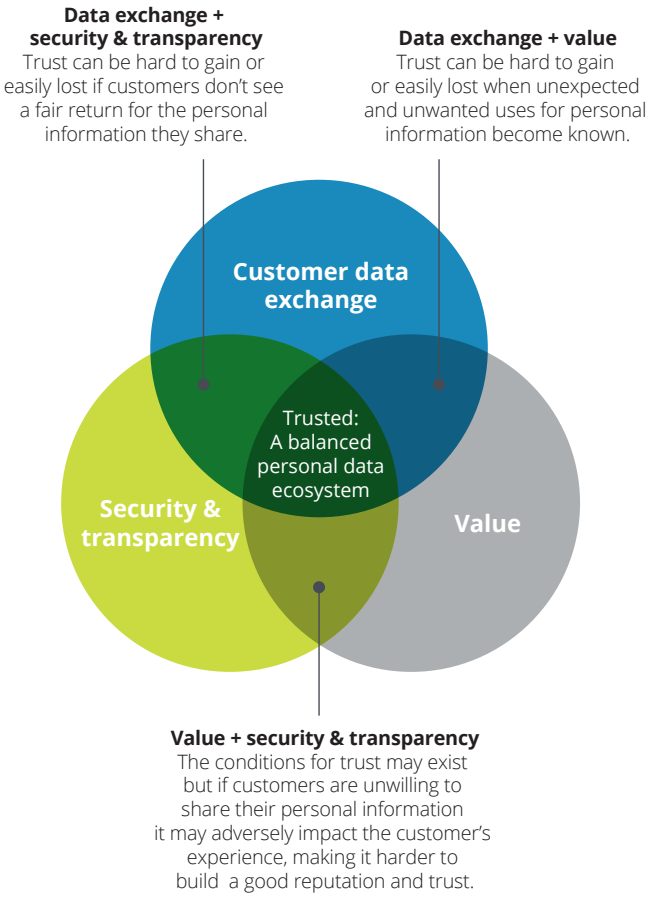


Figure 1: Data Ecosystem

An organisation's response to open banking needs to consider the importance of the information being exchanged, provide transparency over how it's used and shared, ensure the information is secured, and clearly communicate to the customer the value created by sharing the information.

Notes

[2] The Farrell Report's scope was limited to "customer-provided data, transaction data that is stored in a digital form for specific types of accounts held in Australia and product data." Out of scope was "data supporting an identity verification check; any data that would materially increase the risk of customer identity theft; aggregated data; and transformed data". Australian Government, The Treasury, Open Banking customers' choice convenience confidence, Scott Farrell, December 2017 (The Farrell Report) page ix. See also: https://static.treasury.gov.au/uploads/sites/1/2018/02/ Review-into-Open-Banking-_For-web-1.pdf

[3] Deloitte Australian Privacy Index 2018. See also https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.htm

Open banking and privacy today and tomorrow

As Australia moves closer to open banking, participants should understand the current privacy regulatory landscape, global trends, and how it may evolve with the introduction of open banking. There are a number of aspects to consider.

Australian privacy laws: the Privacy Act and the Privacy (Credit Reporting) Code 2014 will continue to apply to the collection, processing, and storage of personal, financial, and credit information in the financial sector. However the Farrell Report recommends that a number of additional or modified safeguards be introduced to "inspire confidence".[4] These proposed safeguards require data recipients to obtain consent at the point of collection, purpose-limited sharing, security when data is stored or transferred, and the right to remedy where requirements have not been complied with. The proposed regulatory framework is still being considered, and is anticipated to be formalised in the coming year, with the first components of data sharing required to be in place by 1 July 2019 beginning with sharing of generic product data.

Currently small businesses with a turnover of less than $3 million are not subject to the Privacy Act. The Farrell Report recommends that all data recipients under open banking be subject to the Privacy Act. Participants that intend to take advantage of open banking including smaller fintechs and 'techfins' will need to ensure that they can comply with the privacy legislative framework.

Comprehensive Credit Reporting (CCR): CCR requires financial institutions to share with other lenders specific credit information that illustrates a customer's positive behaviours. With the first phase originally scheduled to come into effect in July 2018, this mandatory transparency will enhance lender's data accuracy, offering a more complete picture of an individual's credit limits and loan repayment.

Payment Security Directive 2 (PSD2): The European PSD2 came into effect from January 2017 to boost "transparency, innovation and security in the single market" and create "a level playing field between different payment service providers".[5] PSD2 requires several large European and UK banks to allow customers to view and share their personal and financial information with third parties.

UK Open Banking Implementation: To support PSD2 implementation, in January 2018 the UK's Open Banking Implementation Entity (OBIE) released an open banking platform to share financial information. This platform includes a standardised format for sending and receiving data, to enhance the security of banking data shared between financial institutions. The OBIE has also developed prescriptive technical security standards for customer authentication and standards for API specification and encryption.

A multitude of organisations have sprung up as a result of PSD2. This shift of the financial services market is likely to be replicated in Australia, with the introduction of an open banking scheme, with similar privacy issues to be considered and applied.

General Data Protection Regulation (GDPR): the GDPR came into effect on 25 May 2018 and applies to EU-based operations, and Australian organisations which direct products and services or monitor the behaviours of EU-based persons classified as "data subjects". The GDPR contains stringent privacy requirements for the collection, processing, and retention of personal information and grants substantial data subject rights to individuals. This includes the right to data portability, the right to withdraw consent where processing relies on it, and the right to erasure and to be forgotten.

The GDPR's right to data portability will require an organisation, at the request of an individual, to transfer personal information collected from that individual to a selected third party, where the processing is based on the performance of a legal contract or on consent and it is carried out by automated means. Where not technically feasible, the organisation may directly transfer personal information to the individual, or provide access to an automated tool that allows the individual to extract the requested information themselves.

Given that Australia's proposed approach to open banking is broadly aligned to the UK and the EU, Australian organisations should consider the principles from these jurisdictions when developing their privacy frameworks as part of their open banking initiatives. Some fintech organisations have considered adopting the GDPR as the strictest standards applicable to all their customers to future proof the organisation for emerging changes to the Australian privacy regulatory landscape.

Notes

[4] The Farrell Report op. cit., Chapter 4

[5] Comment included in answer provided by Vice-President Dombrovskis on behalf of the commission to a question in the European Parliament, 28 August 2017. See also: http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-003584&language=EN

Privacy issues in the open banking data lifecycle

Individual Rights and data collection

The Farrell report has recommended the creation of a Consumer Data Right in Australia to support the open banking regime. It will allow consumers to control their data, including who can access it and use it, with appropriate privacy safeguards under an augmented Privacy Act.

An individual's consent under open banking must be explicit, fully informed, and able to be time limited or withdrawn, according to the individual's instructions. Permissions cannot be bundled together under a single consent but must be given at a granular level. Consent needs to be truly given. The challenge for participants will be to both provide the right level of detail and to ensure it is easily understood by the customer. As McKinsey points out "There is a fine line to walk: educating and empowering consumers without confusing, scaring, or boring them."[6] The precedent set by GDPR establishes a high standard for consent requirements. Consents must be clearly distinguishable from other matters, be in an intelligible and easily accessible form, and be expressed in clear and plain language.

There will be a mandatory notification requirement by all stakeholders to inform customers about the collection, use, and disclosure of their personal information. This includes how their personal information will be used for marketing and on-sale opportunities. Notifications and consent requests will need to be limited to single screen or page, so that individuals find it easy to understand the implications of open banking, and that consent is informed and meaningful.

Currently Australian privacy law is based on customers electing to opt-out of direct marketing.[7] The Farrell Report recommends moving to an opt-in regime where express consent (which is not bundled with other consents) is required before a data recipient can directly market to the customer.[8] This recommendation goes beyond European's direct marketing law[9] where there are exceptions to the opt-in regime known as 'soft opt-in'. The European law allows organisations to send unsolicited email marketing to an existing customer who has previously purchased, or negotiated to purchase, a similar product or service.

Data use and transfer

The use of personal information under the Privacy Act is limited and based on its purpose – personal information can only be used for the purpose for which is was collected (the primary purpose), or where an exception applies, it can be used for a secondary purpose.[10] Under the GDPR, there must be a defined lawful basis for processing (for example, processed by consent or contract), unless a compatible purpose for intended further processing is identified, with the exception of processing based on consent.

The Farrell Report recommends that privacy protections be modified so that an organisation that receives personal data through open banking can only use it for the primary purpose for which it was collected, unless they can demonstrate a secondary use that is "directly related" to the primary purpose.[11]

The current legal and regulatory environment is not prescriptive on data security. Under the Privacy Act, "reasonable steps" should be taken to protect personal information from unauthorised access, modification, disclosure, misuse or loss. Under the GDPR, organisations are expected to take a risk-based approach to implement appropriate technical and organisational measures, including confidentiality, resilience, integrity, and availability of systems that hold personal information. Australian banks must also consider the Australian Prudential Regulatory Authority's (APRA) prudential standards and guidance on data security.[12]

The Farrell Report has recommended that designated security standards should be set by a data standards body to ensure that open banking participants can safely handle and share banking data.[13] The Report recommends that Australian organisations look to the UK's Open Banking technical specifications, being PSD2 and OBIE's technical standards.

Data senders will have to include in their notification to the customer that their direction has been received and that the future use of their banking data by the nominated third party will be at the individual's own risk.

Banking data must be transferred via secure API-enabled banking services. APIs allow for the secure transfer of information from an organisation's systems to an app or other platform. Key data security considerations include ensuring there are identification and verification processes before transferring personal information, including where there are joint controllers of finances. Transfers of personal information overseas and to third parties must also consider applicable cross-border and third party requirements (including the need for third party processor contractual agreements).

Data storage and disposal

GDPR and Australian Privacy Principles require data to be stored securely and once any legal, contractual or regulatory retention period has expired the data should be destroyed or de-identified. The security controls deployed need to be commensurate with the sensitivity of the data. In addition, GDPR confers on an individual the right to erasure and, in certain circumstances, the right to be forgotten. The Farrell report specifically notes that the consideration of these rights were beyond the scope of an open banking framework, due to its legal complexity.[14]

Open banking will expand traditional banking data flows, placing the customer at its core and in control of their banking data, including their personal information.[15]

Notes

[6] McKinsey & Company, Data sharing and open banking, September 2017. See also https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking
[7] Australian Privacy Principle 7
[8] Farrell Report op. cit., p56
[9] European Directive 2002/58/EC
[10] Australian Privacy Principle 6
[11] Farrell Report op. cit., p56
[12] In particular, CPS 231 on outsourcing, and CPS 234, requiring robust information security practices.
[13] Farrell Report, op. cit., Recommendation 4.8, p64
[14] Farrell Report op. cit., p57
[15] Deloitte, Open Banking, How to flourish in an uncertain future, June 2017, p6. See also: https:// www2.deloitte.com/uk/en/pages/financial-services/articles/ future-banking-open-bankingpsd2-flourish-in-uncertainty.html.

Open banking – privacy rights and wrongs

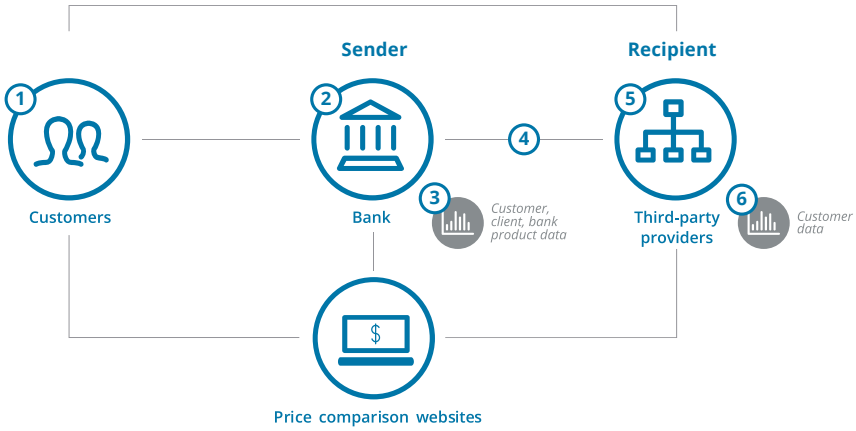


Figure 2: Open banking data sharing

	What needs to occur	What could go wrong
1	The customer initiates the data sharing request	• The consent provided is incomplete and does not include all parties to an account • The customer data sharing request is forged
2	The data sender ensures that they have an express consent which specifies what data is shared, clear purpose, who it is shared with, and how long the data is to be shared, which facilitates transparency	• Express consent is not received • The consent received is incomplete and does not include all parties to an account • The data sender fails to accurately record what data is to be shared, for what purpose, who it is to be shared with or for how long. • The data sender fails to satisfy accreditation requirements
3	The data sender ensures they are able to identify and correctly extract only the customer data that they have consented to share and the data is secure	• The wrong data for a customer is extracted • The wrong customer's data is extracted • The data holder fails to protect the data held
4	The data transfer occurs in the correct format in a secure environment	• The wrong data is transferred • The data is transferred to the wrong party • A data breach occurs during the data transfer
5	The data recipient confirms that they have express consent which prescribes the specific purpose the data can be used for and how long the data is to be held	• The data recipient fails to receive express consent for the data use • The data recipient fails to record the specific purpose for which the data can be used • The data recipient fails to record how long the data is to be held • The data recipient fails to satisfy accreditation requirements
6	The data recipient ensures they are able to identify and use the data only for the purpose for which the customer has given consent and the data is secure	• The data recipient uses the data for an inappropriate purpose for which they have not received consent • The data recipient retains the data for a longer period than that for which have consent • The data recipient fails to protect the data received

Key questions organisations should ask

Open banking cannot operate if customers do not have a high level of confidence that their data is secure and that they are in the driver's seat to determine how their personal information is being handled. And that confidence will not be created without privacy – it demands consideration of individual rights. Its success is driven not only by the businesses involved, but by customer acceptance enticed through a balanced data ecosystem and trust.

The Farrell Report calls out a number of enhancements to the privacy regulatory landscape. The introduction of the GDPR will encourage some financial service organisations to adopt that regulation as the strictest standard for open banking and wider privacy and data protection framework.

When developing an open banking framework organisations should consider the following questions when assessing the adequacy of their privacy safeguards and embedding privacy into its design:

1. Are privacy requirements and individual sentiment being considered early in the design of our open banking solution?
2. Do we have a Privacy Impact Assessment (PIA) process as recommended by the Office of the Australian Information Commissioner and required under the GDPR (where relevant)?
3. Does our data ecosystem balance transparency, security and fair value exchange?
4. Do we understand the privacy risks as well as we understand the benefits of collecting and handling banking data?
5. Are we comfortable that our customer data is complete, accurate and up-to-date?
6. Do we understand the primary purpose for which the data is shared?
7. Do we have the capability to record the customer's consent, including the purpose and the timeframe for which data is shared?
8. Do we have in place a process to assess our open banking framework against individual expectations and not just regulatory compliance requirements?

Last word

Data is valuable, and while privacy requirements may appear to create a challenge for financial institutions, they should be seen as an opportunity and a driver for success. Organisations that provide customers with services they value, demonstrate they value privacy, are transparent about how the data is used and shared, and design a secure portal, will retain more loyal customers, obtain greater customer buy-in and build deeper trust.

This will allow organisations that embrace open banking and tailor their privacy strategies accordingly to unlock the benefits of shared data for their business and their customers.

Contacts

Ilana Singer
Manager
+61 3 9671 5475
isinger@deloitte.com.au

David Batch
National Privacy Lead
+61 2 8260 4122
dbatch@deloitte.com.au

Viv Tannock
Director
+61 403 859 953
vtannock@deloitte.com.au

Series editor

Paul Wiebusch
Partner, Financial Services
+61 3 9671 7080
pwiebusch@deloitte.com.au

MCBD_Syd_06/18_055432