

EMERGING TRENDS IN DATA SHARING AND OPEN DATA A PERSPECTIVE FOR CONSUMER CREDIT PROVIDERS

AN ARCA WHITE PAPER

Authors: David Grafton, Kim Jenkins, Lisa Schutz, Steve Johnson

Additional contributors: Andrea Zannier & Adam Flesch: Oliver Wyman Australia

April, 2017



CONTENTS

1. EXECUTIVE SUMMARY
 2. CONTEXT AND PURPOSE
 3. THE CURRENT FRAMEWORK FOR SHARING CONSUMER CREDIT DATA
 4. EMERGING DATA SHARING AND OPEN DATA PRACTICES BY CREDIT PROVIDERS
 5. OVERSEAS EXPERIENCE: CURRENT POSITION ON OPEN DATA INITIATIVES IN THE UK AND EU
 6. IMPLICATIONS OF WIDER DATA SHARING AND OPEN DATA FOR CONSUMER CREDIT PROVIDERS
 7. GOVERNANCE FRAMEWORK OPTIONS FOR FUTURE OPEN DATA SHARING
 8. CONCLUSION - WHERE TO FROM HERE?
-



1. EXECUTIVE SUMMARY

It has been proposed from many quarters that consumers, credit providers and the economy in general can all derive significant benefits from more open access to data and increasing data sharing. The explosion in data volumes, coupled with new analytical techniques, means that we now have the technological ability to combine and store massive databases and derive insights from a vastly broader and deeper range of information sources than has ever been possible before.

However, the benefits from data sharing will not be realised unless there is a clear governance framework in place that engenders trust and balances commercial interests against those of consumer protections and privacy; a framework that currently does not exist.

The current regulatory regime is not well placed to maximise the benefits that new forms of open data and data sharing can generate. We are entering an era where the pace of technological and business change is running ahead of the regulatory and governance structures needed to maximise the sustainable benefits from broader data sharing.

Overseas experience can provide useful guidance regarding how best to proceed in progressing an industry-wide open data initiative¹. Furthermore, the frameworks, principles and decades of experience entrenched in the sharing and utilisation of sensitive personal credit data provides a useful blueprint to draw on in support of the development of an optimal open data model for Australia.

The key concern is to strike the right balance between consumer interests, such as data ownership rights, consent, privacy protections, data quality and security, and commercial interests including the monetisation of shared

data, reciprocity, fair value exchange, liability of third parties, and permissible purpose. This is especially true with regard to the marketing applications of shared data.

These concerns are not restricted to one credit provider or even a subset of providers; rather, they are concerns that are shared by the consumer credit industry as a whole and need to be addressed accordingly. While this paper focuses on the consumer credit industry, the issues and considerations raised apply equally to other arenas. It is worth noting that, as the range of data types and the range of business entities increases, so too do the risks and complexities.

This paper does not set out to argue the case for, or against, broader data sharing or Open Data initiatives, and the issues outlined are not provided in order to caution against proceeding. Rather, this paper aims to highlight the key issues requiring consideration in the development of an effective and robust data sharing ecosystem.

The absence of an industry-wide initiative to create a self-regulating governance framework raises risks that can arise from the imposition of regulations that may not be sufficiently flexible to fully accommodate current and future commercial circumstances in a rapidly changing business environment.

An industry-wide governance framework that strikes the right balance between commercial interests and consumer protections is urgently required and will be of fundamental importance in ensuring that the maximum benefits from opening and sharing data more widely will be realised; to the benefit of consumers, industry and the economy as a whole.

¹ Useful definitions can be found in The UK Open Data Institute publications: Open Data For Banks (2014); Introducing the Open Banking Standard (2016); Data sharing v.s. Open Data: <https://theodi.org/blog/data-sharing-is-not-open-data>
Open Data definition: <https://theodi.org/guides/what-open-data>
Open Banking: <https://theodi.org/open-banking-standard>

2. CONTEXT AND PURPOSE

The current move towards ‘Open Data’ and expanded data sharing is predicated on the assumption that significant consumer and competition benefits will eventuate. It is facilitated by the vast amount of data now being created (with an estimated 90% of the world’s total data having been generated in the last two years); the availability of low cost technology for combining, storing and processing data; and the power of the latest machine learning and AI data science tools.

There is considerable literature on the general benefits that derive from wider data sharing. Although difficult to quantify with precision, all studies agree that the economic benefits are very significant. For example, work by McKinsey suggests that this could be as much as USD\$3-5 trillion per annum; a global total that includes benefits from public as well as private data sharing².

For the global consumer finance industry alone, the economic upside is estimated at \$210 – 280 billion p.a. deriving from increased innovation and competition, better risk-based decisions, improved access to credit for those currently unbanked, and reduced losses through better fraud prevention. In addition to the hard dollar benefits are further positives in terms of improved customer choice, empowerment and experience, better tailored products and more relevant target marketing.

Historically, banks and other financial institutions have made use of their own customer databases, and the sharing of defined sets of credit data via credit reporting bodies, to automate and improve credit decisioning, ensure responsible lending practices, and to drive target marketing activities, although the latter purpose is not permitted here in Australia. Today, there is a gathering trend to share, combine and provide more open access to information that may come from, or be provided to, a wide range of parties *other than* the credit provider (“CP”).

Such a form of data sharing goes far beyond the traditional “peer to peer” data sharing activities that are well established via credit reporting bodies (“CRBs”) in making a consumer credit assessment. Some potential examples include the open interbank exchange of transactional information to, theoretically, enable consumers to more easily switch banks, the use of social media data for credit assessment, and the pooling of large datasets (loyalty programs, credit card transactions and supermarket shopping data) for marketing purposes.

Against this background of rapid technological and business change, there is growing recognition that the regulatory environment in Australia is not adequate to manage the new initiatives and business models emerging in the “data economy”. The Productivity Commission for example has explicitly recognised the need for “fundamental and systematic changes”³ in this regard, including a new Data Sharing and Release Act and a set of “comprehensive rights” for consumers that will maximise the benefits from data sharing whilst retaining key consumer protections. This is a critically important balance to strike and a theme that pervades much of the discussion that follows.

² McKinsey Global Institute (2013) Unlocking innovation and performance with liquid information

³ Australian Government Productivity Commission (2016) Data Availability and Use Draft Report

This paper seeks to contribute to this debate, *specifically from the perspective of Consumer Credit Providers*. It does not argue the case for or against broader data sharing in the credit arena, but rather, sets out to explore some of the main issues and dilemmas involved in doing so, including:

- » A review of the current data sharing governance framework (section 3) and emerging data sharing activities being undertaken by CPs (section 4)
- » Referencing some recent international ‘open data’ initiatives and considering how these examples might assist in informing Australian CPs in the new data sharing environment (section 5)
- » Discussing some key consumer and CP issues arising from such activities and likely future developments (section 6) including
 - Consumer rights and protections (section 6.1) and
 - Commercial interests and other considerations for CPs and third party agents (section 6.2)
- » Considering how the mature frameworks that have been developed in support of effective credit reporting environments, both here and overseas, may provide a useful ‘blueprint’ for informing the development of models for a broader “open data” ecosystem (section 7)
- » Suggesting a series of “next steps” to move towards an industry-led view of how open data and data sharing should operate (section 8).

The intention is not simply to contribute to the general debate, but to highlight key issues of relevance for the consumer credit industry, and to encourage a proactive and collaborative process for developing an appropriate framework for the sector.



THE PRINCIPLES AND FRAMEWORKS THAT EXIST IN THE CREDIT REPORTING ARENA PROVIDE A RELEVANT AND USEFUL POINT OF REFERENCE WHEN CONSIDERING OPTIONS AND ISSUES REGARDING A BROADER DATA UNIVERSE



3. THE CURRENT FRAMEWORK FOR SHARING CONSUMER CREDIT DATA

A mature legacy of data reporting and utilisation practices exists in the arena of credit assessment and management. This presents a useful point of reference for considering potential principles and frameworks relevant to the newly emerging data sharing and utilisation debate.

Data used for credit purposes is personal, which means it can and must be identified and linked, accurately and directly, to a specific individual. It therefore carries an additional burden of protection on behalf of the consumer in terms of data quality, accuracy, timeliness, security and any potential downstream use.

Paramount in ensuring accuracy is the method used to match information from different sources to the correct individual. This is not a trivial task and the credit bureaus, for example, have invested considerable sums over many decades to ensure that matching is as accurate as possible. In the absence of a unique identity number (such as a National Identity Number or the US Social Security Number) reliance is placed on information such as name, address and date of birth which greatly increases the complexity of the matching process in view of the many different ways that this information can be structured and spelled.

Part IIIA of the Privacy Act sets out clear obligations and restrictions on credit providers. It provides consumers with clear rights, in terms of privacy principles; data accuracy and completeness; advance consent; restrictions regarding permitted use of data; and consumer rights of access and data correction, all of which demand the most rigorous approach to data matching for credit purposes. Similar protections are likely to be required in a new world of broader data sharing.

Many of the issues being discussed today in relation to a framework for data sharing and open data have been given close consideration

in the development of the current consumer credit regulatory regime and data sharing practices that underpin credit providers' use of credit bureaus.

In Australia, credit assessment data and credit history information have been shared for over 50 years, albeit in a highly regulated "negative" reporting environment. The current and familiar process of data sharing under conditions of reciprocity that underpin credit providers' use of credit bureaus, and the principles and frameworks that exist⁴ provide a relevant and useful point of reference when considering options and considerations regarding a broader data universe and/or a broader set of purposes.

Of particular relevance to the current debate on wider data sharing is the governance framework which relies on an overarching legislation, supported by regulations and further strengthened by an industry-developed self-regulating code of conduct that includes data standards and "give to get" reciprocity rules. In addition, the current framework provides for clear consumer rights regarding access rights and complaint and correction mechanisms. Marketing uses of the data are highly restricted. Data security protocols and protections are strong, and instances of data breaches are extremely rare. The structures, principles and decades of experience enshrined in this framework have much to offer the current debate on data sharing.

A key issue to consider is the adequacy of this framework relative to the new forms of data sharing and open data initiatives that are now emerging and, while not perfect, there is merit in taking the current framework as a starting point 'blueprint' to work from in developing a broader data sharing model.

4 These include legislation, the Credit Reporting Code (CR Code), the Principles of Reciprocity and Data Exchange (PRDE) and the Australian Retail Credit Reporting Data Standard (ACRDS) as well as familiar and accepted business practices and processes such as methodologies for developing, testing and monitoring scorecards and policy rules.

4. EMERGING DATA SHARING AND OPEN DATA PRACTICES BY CREDIT PROVIDERS

Credit providers today are involved in data sharing and are likely to find increasing interest from other parties in the value of the credit data they hold.⁵ Credit data is necessarily of high quality, is relatively complete and up to date, is referenced at a personal level, is highly predictive of other risk and marketing behaviours and is therefore extremely valuable.

Some credit providers share their own credit data directly with internal insurance divisions in order to improve underwriting, especially for auto insurance. Credit data is also used for product development, market research and marketing purposes such as customer segmentation codes, propensity models and permitted direct marketing activities. This trend is likely to continue and there is increasing interaction between credit and marketing departments to maximise the use and value of credit data for permissible marketing applications.⁶

Data may be shared at the individual level, which is where most value lies, or can be shared in a depersonalised or aggregated form such as at a metadata or postcode level. When aggregated, the Privacy concerns are less acute, but the practical value of aggregated data is generally much less than the data at a granular, individual level. Accordingly, it is to be expected that most demand will be for individual rather than aggregated data sharing.

A further and bigger step, and a challenge for the current governance framework, is to broaden the universe of data used in support of marketing insights, trade area analysis and product development by combining credit data with other large databases, e.g. loyalty schemes, supermarket shopping data and residential property information. Often this will be done

via a third party which may undertake matching, depersonalisation, data storage and analytics to derive insights. Such initiatives require great care in terms of accurate matching, consents and consumer protections.

Credit data may itself be enhanced by combining with non-traditional sources of information that may improve credit assessment, for example the use of social media data, payment data (e.g. from non-traditional payment gateways such as PayPal or Apple Pay), utilities, TV rental and tenancy information. This is already occurring in other countries including the USA, and, again, raises questions about consumer rights.

The new world of data sharing involves a wide range of activities and players, as shown in the table below. Organisations participating in the data sharing and utilisation ecosystem are likely to be operating across multiple roles and need to consider carefully the implications that arise from each activity that is undertaken.

⁵ Credit data here is taken to mean personal identity, financial details, transactions, application and behavioural scores, bureau data and credit performance information.

⁶ The authors of this paper have all had personal experience of being called to assist a broader audience in understanding and considering the right way to balance the trade-offs involved in data sharing – particularly in the marketing context

DATA ENTITIES	WHO PLAYS THIS ROLE - EXAMPLES	DESCRIPTION	KEY CONSIDERATIONS FOR A CREDIT PROVIDER
Data subject	Applicant for credit	Data subject is either an individual (key focus of this paper) or an entity.	The consumer issues of consent and fair exchange as documented in the paper – the CP needs to review data sharing from the data subject's perspective – do they understand the data sharing value chain and consent to it.
Primary data collector	CP via application form	This entity is generating or collecting data about the subject.	The primary data collector represents the point in the value chain where consumer consent must be obtained – this is where the issues arise of how permission can be obtained in a manner that data subjects understand, how the Privacy Act's requirement of reasonable expectations for downstream use applies and how to deal with potential new uses for data thought of after permissions have been gathered will be addressed. As a CP the examination of permissions in light of the rest of the value chain is crucial.
Data contributor	CP supplying data to a credit bureau. Credit department supplying data to marketing department. Or, third parties such as Yodlee and others might be providing data to CPs.	The entity providing data into a data exchange.	CPs need to understand data contribution both as a contributor (leveraging their primary data collector status) and a recipient (in their role as a data user). Contributor: The CP's credit team might be overseeing the contribution process – as is the case of credit data reported to CRBs – but another department (such as marketing) might be running a data sharing program without involving the credit team.
Primary data user	Credit Provider	The entity using the primary data in its original form for a purpose clearly understood by the data subject or entity that agreed to share it	This is the easiest area for permission – because the user expressly understood they shared data in order to get either a better service or a better product or gain access e.g. agreeing to share credit data. Issues of consent and permissible purpose are key but generally well handled by existing processes.
Data user / recipient	Wide possible range including CP and third parties including parties outside of financial services.	A user of the end product of the data, typically in a modelled or aggregated form of some kind but can also be in its raw (albeit digitised) form.	If a CP has contributed data for which they were the primary data collector, how do they monitor, on an ongoing basis, downstream use and compliance in terms of permissions (would the consumer think they had given permission) and security (even de-identification is not necessarily sufficient)? Likewise, if CP credit teams access data for responsible lending that was not collected for that primary purpose, how do they ensure that any third parties they use recognise the privacy and security interests of the data subject and primary data collector? Recipient: Alternatively, if a data user is obtaining the data via third parties, a number of questions arise for the CP. If the data is being accessed, for instance, via “screen scraping” technology, the chances are the primary data collector is unaware of the data use (thinking the data access is from the data subject) and has no direct line of sight to the data subject to know it is a genuine request and not a hack. The importance of portal security in protecting the banking credentials of consumers is critical, as is ensuring that such portals operate in a manner consistent with the data subject's obligations not to disclose their credentials to another party.

DATA FACILITATORS			
Data managers	e.g. CP, Amazon, IBM.	In some cases, a third party will provide the data management services and in turn they might outsource physical infrastructure (storage, transmission) which creates complexity.	Data principals will often outsource tasks to data facilitators. CPs will take this role in-house in most cases, but how do they get full visibility to the third party firms involved in the value chain and manage issues over security, data quality, liability and redress? These issues are constant across all the firms involved in data facilitation.
Data stores	CP, various third parties including Amazon, IBM, Microsoft.	The environment in which data is stored or the entity doing the storing. All other roles in the ecosystem rely, to some extent, on data storage. This may be temporary or long-term and many variations exist in terms of infrastructure.	Questions for CPs to consider: levels of normalisation; physical versus “cloud”; onshore vs offshore; encrypted or open; identified or de-identified, as well as protocols regarding access and broader security. Downstream data receivers’ security may be less rigorous than originator standards. Where does the CP’s role as a data principal end in assessing the integrity of the value chain?
Data transmitters	CP itself, various third parties including Amazon, IBM, Microsoft.	Examples include the encryption tools and services that have evolved to handle e-signatures, encryption and, of course, new entrants such as blockchain solutions.	The CP’s role in assessing these data transmission service providers and methods is again unclear. Does their job stop when the data leaves their environment? And yet permissions at the start of the value chain need to carry through to the final data consumption point. There are a range of specialist third parties that can be involved in providing encryption and other services related to transmission of data.
Data security – audit.	Examples include Big 4 accounting firms and various niche IT security firms.	Additional to the physical infrastructure are the security specialist firms that audit the data facilitation infrastructure	CPs can probably use this stage in the process to achieve more control on the value chain if a broader audit was required than pure IT security for value chain participants. Currently, the audit focus of the data security firms tends to be on physical data security rather than privacy, which tends to be more the province of in-house legal/compliance teams at the primary data collector/data user stages of the value chain.

INSIGHT CREATORS			
THE ROLES BELOW ARE ALL COMPONENTS OF THE INSIGHT END OF THE VALUE CHAIN - THEY CAN BE ALL PROVIDED BY ONE SERVICE PROVIDER BUT ARE OFTEN SPLIT.			
Data matchers	Credit Bureaus CPs third parties e.g. Data Republic, Quantum.	Data matching. Often accompanied by post matching processes de-identification and aggregation.	Data matching is a vulnerable part of the value chain to the extent that two sets of data, with personal information exposed, are joined. While there are organisations which offer algorithmic data matching (meaning that the data doesn’t have to be physically co-located to be matched) access to the algorithm provides the capability to match and thus algorithm security is a key factor. CPs need to be aware of the issues and be able to evaluate on an informed basis. Matching accuracy is also a factor to consider. Probabilistic matching is usually required due to natural variants in how names and addresses are presented, but creates accuracy issues.
Data aggregators (and de-identification)	CP or third parties.	Preparing data for analysis often requires aggregation.	Data aggregation and de-identification (if the data is to be analysed at the individual data subject level) involve skill both in statistics and security. Permissible purpose and consent issues arise for CPs to consider.
Data analysts	As above.	Tends to be more historical review of data trends, snapshots. Often referred to as Business Intelligence.	The key distinction between data modelling and analysis is that analysis does not attempt to predict. As soon as prediction is required historical data and outcome samples are required. This requires more data and more time specific data.
Data modellers	As Above.	This is where data is used to predict future outcomes, based on historical observations. Credit risk models are an example (as are marketing propensity models).	Concerns here for CPs would include permissible purpose, consent and model accuracy. The latter is particularly a focal point because predictive models are used to make forward looking decisions which can affect data subjects. The classic example for CPs is predictive credit models. Data analysis for a CP would include historical monitoring of bad rates for a credit portfolio.





5. OVERSEAS EXPERIENCE: CURRENT POSITION ON OPEN DATA INITIATIVES IN THE UK AND EU

When considering emerging data sharing activity, particularly as it relates to the sharing of statement and transactional data between credit providers to make account switching easier and to stimulate competition, it is instructive to look at initiatives already under way in the UK and the EU.

The UK is seen as a leading example in encouraging wider data sharing in general, and in open data initiatives in the banking sector in particular. These are designed to stimulate competition to the benefit of the consumer by making it easier to switch banks and obtain a better deal. In a similar vein, the Australian Productivity Commission is recommending that consumers be provided with a digital, machine readable copy of their data which can be used to elicit better offers from competing service providers, especially banks.

5.1 Open Banking initiatives in the UK

In the UK, there is considerable momentum towards the adoption of open APIs (Application Programming Interfaces) as the means by which consumers can access and transfer their data in a digital format. The UK has been a forerunner in launching Open Data and Open Banking legislation, sooner than many other markets. The UK HM Treasury Open Banking initiative aims to improve competition and consumer outcomes by giving customers the ability to share their transaction data with third-party providers (3PPs) using an open API standard for UK treasury. Problematically, the associated regulations are applicable only to the 9 largest banking institutions in the UK.

An Open Banking Working Group was established by the UK Government in August 2015, giving it the remit to design a detailed framework for the development of an open API standard in the UK. In February 2017, the Retail Banking Market Investigation Order formally established an Implementation Entity funded by the Banks, comprised of

bank and regulatory representatives, to agree, implement, and maintain the open banking standards.

The UK financial community – in the form of the Open Banking Working Group – is playing a proactive role in defining the standards and governance framework for open banking, including:

- a) To create an open standard without requiring bilateral arrangements between a third party and each data attribute provider
- b) Data standard definition: rules by which data are described and recorded
- c) API Standard: specifications regarding design, development and maintenance of an open API
- d) Security Standard: security aspects of the API specification
- e) Governance model to operationalize the Standards
- f) Developer resources to enable third parties to discover, educate and experiment

Lessons learnt from the UK experience to date have highlighted the importance of a proactive industry-led approach to informing and working with regulators in developing an appropriate, flexible and effective framework for the enablement and regulation of the 'Open Data' initiative. In addition, a failure to ensure effective and early broad-based consultation and engagement, not only of stakeholders within industry, but across the range of key interested parties, has been highlighted as an early misstep by industry in the UK.

A report released by the Open Banking Working Group⁷ states that banking customers (individuals and businesses) need to understand their responsibility for

⁷ See <http://banknxt.com/55745/uk-open-banking-api-framework/>

informed customer consent and ensuring their data is protected. This is problematic in light of losses arising from social engineering-enabled identity theft and impersonation, which is an emerging global fraud threat. The report acknowledges that it's likely that cybercriminals will specifically focus on the open API as a new attack vector⁸.

Other markets (in the EU and beyond) have begun to implement aspects of an Open Banking standard, but none has produced a definitive outline of such a standard, let alone a roadmap for its implementation.

5.2 The EU PSD2 initiative

PSD2 is a European Directive that seeks to drive increased competition, innovation and transparency across the European payments market (Ref Accenture). The account access provisions of PSD2 require Euro-area banks to provide open access to customer information where third parties have the explicit consent of the customer.

It requires banks to implement common APIs that allow "third party providers" to securely access a bank customer's online account and payment details, given consumer consent.

Although designed primarily to facilitate competition and disruption in the payments market⁹, its provisions also enable consumers to transfer their data from one bank to another, or to a non-bank that is accredited by an EU member state (for example Google or Amazon). This has major implications for existing banks and has been described as the biggest change in banking in 7,000 years.

Some concerns arising from the UK and EU experience have direct relevance to Australia. These include what some see as overreach on the part of the regulators, imposing a very aggressive timescale for change; not considering some of the financial

implications arising; restricting data sharing to statements only; focusing the regulation on just the nine largest banks (in the case of the UK); and, crucially, not clearly defining success criteria from day one, and not involving consumer groups until very late in the process.

There are further issues over whether API-based data sharing would actually lead to increased switching and competition. For example, over \$750M has already been spent by the UK banks on making switching easier¹⁰ but, despite this, results have shown a marked **decrease** in switching over recent years. Similarly, in Hong Kong, the introduction of regulations regarding number portability designed to make it easier for customers to switch between telcos actually served to further concentrate the industry rather than the reverse¹¹.

The question of whether the underlying objective is increasing diversification of the market or enabling easier switching is a key distinction. Mandating mechanisms such as open-APIs and number portability may solve the latter but actually reduce competition if a few players in the market are clearly offering better products and services by making it easier for consumers to leave their current service provider. As the above examples show, easier switching is not synonymous with greater supplier diversity or wider spread of accounts.

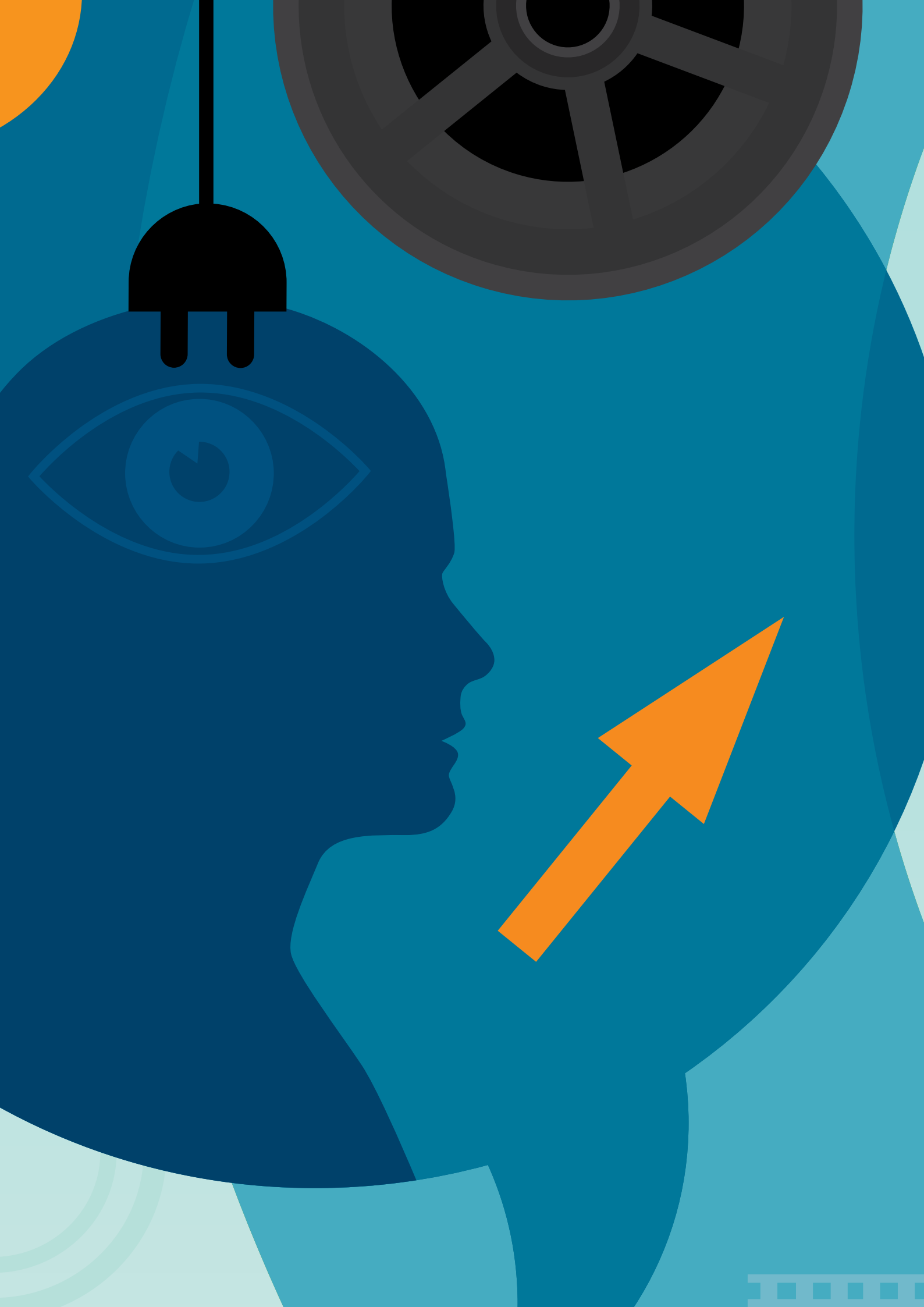
Fundamentally, however, in Europe and the UK regulators stepped in to take action because there was no action being taken by industry. This is a very important lesson that all CPs should be aware of in this jurisdiction.

⁸ See <http://banknxt.com/55745/uk-open-banking-api-framework/>

⁹ <https://www.accenture.com/au-en/insight-psd2-opportunities-banks>

¹⁰ ABA Open Data Symposium (2017) Mike Booth, Director, Advisory Services, Ernst & Young

¹¹ <http://www.chicagobooth.edu/research/workshops/marketing/archive/WorkshopPapers/mshi.pdf>



6. IMPLICATIONS OF WIDER DATA SHARING AND OPEN DATA FOR CONSUMER CREDIT PROVIDERS

Data sharing activities need to be considered in the context of commercial and consumer benefit set against the need to maintain both consumer and commercial rights and protections. The key issue is the balance that needs to be struck between the two.

This tension is not unique to credit data – a recent Harvard University paper on Open Data initiatives in cities raised the exact same point:

“Cities today collect and store a wide range of data that may contain sensitive information about residents. As cities embrace open data initiatives, more of this information is released to the public. While opening data has many important benefits, sharing data comes with inherent risks to individual privacy: released data can reveal information about individuals that would otherwise not be public knowledge”¹²

The Productivity Commission is very clearly aware that there is a danger that there is “scope for Australia to forgo much of the value” (of data sharing) due to the “misconception that denial of access would minimise risks”.

The sections that follow set out some key issues and dilemmas that arise in this context and deserve consideration as organisations consider participation in a broader ‘open data’ ecosystem and as industry (along with government and regulators) consider the development of overarching frameworks and policies.

6.1 CONSUMER RIGHTS AND PROTECTIONS

Central to the sharing of, and open access to, personal data is the need for consumer protection. In this regard, in any data sharing regime, the question of ownership of data and the rights of an entity to share or distribute a consumer’s data to another, needs to be considered. This and a number of related issues are examined here.

6.1.1 Personal data ownership and IP rights issues

The distinction between personal data and personal ownership of data is a subtle but critical one. Certain data elements such as name, date of birth, age and gender are obviously intrinsically ‘about’ a person and can be considered to be ‘owned’ by that individual. Ownership of data generated by a person through their use of a particular entity’s products and services is not as clear cut.

For example, a recent 2017 Federal Court ruling¹³ regarding a case brought by the Privacy Commissioner against Telstra ruled that data relating to a consumer’s use of the service is metadata belonging to the service provider and not personal information about the individual.

The right of access is different to the right of ownership and today there is little clarity as to what data is “owned” by the consumer (and, if owned, what downstream rights attach); and what data is “owned” by the credit provider.

The ‘comprehensive right’ proposed by the Productivity Commission of consumers to access and make use of their personal data needs to be balanced against the service provider’s right to protect their commercial interests and intellectual property¹⁴

Furthermore, the question of when it is or is not appropriate to charge the consumer a fee to cover the costs of providing the information or

¹² Ben Green, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. Open Data Privacy (2017). Berkman Klein Center for Internet & Society Research Publication <https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf?sequence=5>

¹³ Federal Court ruling in the case of Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017), File Number VID 38 of 2016 regarding the appeal from Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991

¹⁴ The proposed ‘Comprehensive Right’ for consumers is intended to provide the right to view, edit and correct information and to be advised of any disclosure to third parties. It also will provide improved rights of opt-out and will give consumers the right to access to a machine-readable copy of their data so that information can be supplied to a third party in an automated manner.

for the estimated value of the information itself has not yet been fully explored, although in the EU it is clear that no fees to the consumer are envisaged.

The boundaries of a consumers' rights to request access to 'their' personal financial services data have not been clearly demarcated. This becomes further complicated when considering the boundaries of a consumer's right to transfer data from one service provider to another, request deletions or corrections of data, or request detail regarding how their data is being used.

6.1.2 Opt-in issue

On the premise that consumers do have a right to determine the use of their personal data, it follows that consumers should have the right to opt-in or opt-out whenever their data is transferred from one data agent to another.

This right would thus apply whenever their data is transferred or on-sold for a specific purpose that is identifiable and targetable directly back to the consumer as an individual. The right of a credit provider to use credit information is restricted by the Privacy Act to purposes that a consumer would "reasonably expect" that data to be used for. Even so, provision of such data to a CRB requires the consumer's opt-in consent.

Any purpose outside of that expectation would likely require further explicit opt-in consent. However, opt-in processes are problematic in that, unless taking place at the point of capture, e.g. at the time of credit application, very low opt-in return rates would be likely to be obtained. In addition, the consumer would need to be in a position to give "informed consent" which would require a high level of transparency over current and future use at the time consent is sought.

This presents challenges given that not all potential uses for the personal data and personal data value added products are necessarily evident at any specific point in time. Upfront

opt-in mechanisms therefore suffer by either being overly restrictive - hampering possible future business needs and opportunities, or overly broad - and thus not providing the consumer with any real transparency or protection.

6.1.3 Opt-out issue

Given an assumption that consumers should have the right to opt-in or opt-out of non-mandatory transfer and uses of their personal data¹⁵, opt-out mechanisms, like opt-in mechanisms, also present challenges. These include the challenge of ensuring that consumers are provided adequate notification of intended use in order to be in a position to opt-out; the need for transparency; the ability to maintain records and audit trails to ensure that permissions are appropriately matched to records and uses; and the commercial risks of very high opt-out rates.

As noted by Grace Brasington¹⁶, VP global banking and financial markets at IBM, "people will trade privacy for convenience". Avoidance of high opt-out rates requires an overt appreciation by the consumer of the convenience or utility that they perceive they would receive as a trade-off against the use of their personal information. As with opt-in, there are clear challenges here in relation to how best to provide transparency and enable a consumer to give "informed consent". A standard table of intended data uses with a tick box against each could be an avenue worthy of discussion, but the issue remains that not all future uses of data will be known at the point in time that the consumer gives or withholds consent.

To address opt-in / opt-out processes, effective, user-friendly mechanisms are needed to enable customers to configure and manage data use and sharing settings on an ongoing basis. Precedents already exist for this in a variety of contexts, including social and business networking applications.

¹⁵ This would exclude, for example, credit data reported by credit providers to credit reporting bodies and metadata collected by all Australian telecommunications companies for provision to law enforcement agencies upon request.

¹⁶ Grace Brasington, Vice President of Global Banking and Financial Markets at IBM. Panel discussion at ASIC Conference 20-21 March, 2017

6.1.4 Profit-share issue

The use and monetisation of consumer data brings into question the issue of whether and how customers should have the opportunity to share in the profit arising from the monetisation of their data.

An argument could be mounted to the effect that if the data belongs to the customer, then there should be equitable reward back to the consumer from the company that is monetising that data asset. In turn this then raises the question of what share in the value chain should return to the consumer and how would fair value be assessed?

It is of interest to note that in the USA, AT&T offer a 30% discount on bills if a consumer agrees to AT&T on-selling an individual's data; so the value would seem to be high. Conversely, one of Australia's telcos calculated that the losses they would incur through erosion of consumer trust was significantly greater than the potential upside that may be derived from the monetisation of customers' personal telco data.

Sharing the value upside with consumers may prove an important factor in optimising a sustainable expanded data sharing and utilisation ecosystem. The value upside shared may be in a monetary form or via some form of 'utility' (in the economic definition of the word). For example, Facebook, Google and many other sites have business models that include the monetisation of consumer data as a core element. They do not pay for this but provide a service free of charge to consumers which is valued in itself.

Market forces are efficient mechanisms for dealing with such issues. Consumers are by now familiar and relatively comfortable with the notion "If you are not paying for it, you're not the customer; you're the product being sold"¹⁷. Individuals will each have different value judgements and levels of comfort with the use of their data - finding the right balance for its own desired target market is key for organisations seeking to utilise or directly monetise their customers' data.

6.2 COMMERCIAL CONSIDERATIONS

In addition to consumer protections, CPs need to consider a range of operational and commercial issues that arise from data sharing. These include the terms of data sharing (including, but not limited to, questions of reciprocity and fair value exchange), data security, liability, the risks of data re-identification, and how to operationalise an

open data exchange that meets the needs of consumers and commercial entities, delivers against any regulatory requirements in this regard, and protects the integrity of the overall system.

6.2.1 Reciprocity issues and fair value exchange

When CPs share credit data amongst themselves, reciprocity principles are the long-standing and well-guarded cornerstone of an effective and equitable credit reporting ecosystem. However, while this is relatively (though not entirely) straightforward when similar entities such as credit providers sharing the same types of data are concerned, it becomes less clear and straightforward when expanding the boundaries to include a broader range of market players and potential participants in the data ecosystem. When the concept of data sharing is broadened beyond credit data for credit purposes, complexity increases significantly and the asymmetry of value exchange suggests a price mechanism model may be needed.

In many markets with a mature credit data sharing environment, Credit Providers have adopted the reciprocity principle as the basis for the exchange of credit data amongst participants. This "give to get" principle underpins the integrity and sustainability of the credit reporting system by ensuring a 'synergistic' rather than 'parasitic' relationship between participants. It is also a closed system in that only credit providers are permitted, under the provisions of the Privacy Act, to access this data and only in support of underwriting their credit decisions.

Even so, during the initial phase of transition from negative only to positive, or comprehensive, data sharing, it is common for larger market share participants to consider that they may give more than they get compared with smaller participants and this has been seen to slow adoption by major players in several markets around the globe.

Perceptions around such value gradients will likely occur when other forms of data sharing are being contemplated and, furthermore, are expected to become even more complex when considering inherently asymmetrical data assets. This is where issues of "type" or "quality" of data are added to the issue of "volume" when assessing value to be exchanged. Especially when the data sets to be shared or exchanged are fundamentally different.

¹⁷ The origin of this quote is not certain but is generally attributed to a comment made by Andrew Lewis (aka blue_beetle) on MetaFilter.com

For example, given increasing innovation and intermediation in the payments ecosystem, should payment gateways such as PayPal and Apple Pay have access to credit data to support anti-money laundering processes, and be required to contribute payment data for use by credit providers in support of their credit and serviceability assessment processes?

Direct reciprocity models are very helpful in the context of credit reporting but are potentially not universally applicable. CPs will increasingly need to consider what fair exchange looks like, and how a market for such data might operate, in a world where the uses of the data they collect are far broader than their own purposes would contemplate.

In the case of an Open-API system for the exchange of statement data, a reciprocal model may well provide an appropriate and effective framework – access to the system being predicated on an organisation also supplying statement information to the system as required and through use of a common data standard. This would, for example potentially avoid the asymmetry arising in the UK where only the 9 largest financial institutions are being compelled to provide open-API access, but does not circumvent potential issues relating to disparities arising from market share differences between the participants or the question of how new entrants will be incorporated into the system.

These and several other questions will require careful consideration in order to ensure the development of a robust and equitable ‘open data’ framework.

6.2.2 Security issues

Security protection to prevent the loss or misuse of the data that is being shared is the biggest single concern of CPs in relation to data sharing. Comments made by the CEOs of the major Australian Banks at the Senate Estimates hearings held during March 2017 have emphasised the need for a trusted framework for the exchange of consumer data, with data security concerns emphasized as paramount.

In particular, the risks to both the disclosing and receiving parties involved in transferring a customer’s personal data to a third party are seen as very high. Banks, in particular, have invested heavily in security, not least to engender trust without which it is unlikely that consumers would be willing participants in any scheme to exchange data. This foundational

concern requires a new control framework that will include data standards, the identification of “trusted entities”, security protocols, process monitoring, and auditing to ensure compliance.

6.2.3 Liability issues

The issue of where liability would rest should personal data become corrupted, lost or intercepted when being transferred from one entity to another at the request of a consumer warrants consideration. The potential for data breach penalties and reputational impacts present material potential risks. Recent comments at the FinTech Conference in Sydney on 20-21 March 2017 by ANZ CEO, Shayne Elliot, that one quarter of the attacks on his bank related to data, clearly illustrates the potential scale and importance of this issue.

A further key issue is how to assess the relative liability that attaches to the disclosing party and the receiving party in terms of data accuracy and which party has liability, in the event that customer harm eventuates; for example, in the event of ID takeover, or data errors. This was seen as an extremely complex issue to resolve at an ABA workshop on Open Data.¹⁸

6.2.4 De-identification and re-identification issues

Given the less acute privacy concerns over depersonalised compared with personal data, there are data sharing activities that use depersonalised information. The replacing of personal identifier information with some form of key or token (“tokenisation”) allows data to be stored in a way that eliminates some of the risk. For example, in the event of a data loss or theft, the absence of any personally identifiable data protects those individuals from the privacy and data security issues that may otherwise have accompanied such a breach.

However, this assumes that the data is not able to be re-identified and, furthermore, does not obviate the need for consumer consent that their data be shared, stored and used in this way in the first instance. CPs need to ensure that the release of depersonalised data has the appropriate permissions and satisfy themselves that it is not possible to be re-identified.

There are examples where depersonalised data has been able to be linked back to individuals – a classic example being the release of postcode-level datasets by Baltimore City Council¹⁹ and the recent publicity concerning the “invited reverse engineering” of telco metadata that

¹⁸ ABA Open Data Symposium (2017) Michael Green SC – Level 22 Chambers

¹⁹ Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. 2017. Open Data Privacy (2017). Berkman Klein Center for Internet & Society Research Publication <https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf?sequence=5>

enabled a frighteningly accurate insight to the minutiae of an individual's personal life²⁰.

6.2.5 Non-credit data used for credit purposes

Non-credit data may be derived from a variety of sources such as bank statement information (such as savings and current accounts); transactional data (including charge, credit and debit cards); payment gateway data (such as PayPal); so-called "public domain" information sources including Social media (such as Facebook, LinkedIn, Twitter, dating websites and so on) and government data sources (such as ATO and Centrelink).

The use of non-credit financial data such as bank statements and transaction information can add significant value when considering ability and propensity to repay a credit obligation and to satisfy responsible lending obligations. However, this data offers a very detailed and personal view of an applicant's private life.

Awareness of privacy considerations is particularly key when considering and communicating reasons for credit decisions on joint credit applications where sensitive information may come to light regarding one or other of the applicants.

A balance needs to be drawn in endeavouring to ensure that adequate serviceability assessments are carried out in support of responsible lending obligations versus avoiding overly intrusive forays into the applicant's private life. In addition, the extent of the compliance burden that may arise needs to be taken into account.

This is an area where industry and regulators will need to work closely together to strike the optimum balance.

6.2.6 The public domain issue

There appears to be a widely-held assumption that it is permissible and appropriate to use personal information that exists in the public domain such as social media information, as input to predictive models, including score cards. However, consideration needs to be given to whether the purpose intended for such information (for example, communicating with family and friends) is consistent with its use for alternative purposes such as credit assessment, and whether the 'owner' of that data could have reasonably expected that it would be used for the alternative purpose contemplated.

Furthermore, if consumers became aware that their public data was being used for credit assessment, this may change some individuals' willingness to post accurate information, or even incentivise deliberate manipulation of information in order to mislead, thus contributing to a degradation of the predictive value of such data over time.

Careful consideration of applicable language in the Privacy Act as well as ethical and reputational issues is needed.

6.2.7 Credit data used for non-credit purposes

Non-credit purposes include the design and execution of targeted marketing campaigns; market segmentation and research; input to government and local government infrastructure and services planning processes; insurance underwriting and more. Currently prohibited in Australia, but permitted in some other jurisdictions with mature positive credit data sharing environments (including the US, UK, South Africa and others) is the use of credit data for non-credit related purposes.

Credit files, specifically account and profile header data such as name, address, date of birth and contact details are a valuable and reliable source of demographic information at the individual consumer level. In some countries (e.g. the USA), the full credit file may be used, whereas in others only specific data elements are permitted to be used depending on the intended purpose.

20 <http://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626>

The current debate about wider data sharing is likely to reopen discussions on what is, and what should be, permissible in Australia. Currently, the Privacy Act stringently limits data utilisation, setting tight controls around what data may be shared and by which types of organisations; which organisations are permitted to access this data and the purpose for which credit data may be used. In a broader context, as contemplated for example by the Productivity Commission's envisaged "Data Sharing and Release Act", the questions of what data is permitted to be shared, the purposes for which data may be used and other considerations, some of which have been flagged in this paper, will need to be addressed.

There is particular sensitivity regarding the use of credit data for marketing purposes. This was a major area of debate in the development of the 2014 Privacy Act and almost all CPs were opposed. In particular, the larger CPs could not see any benefit in providing smaller competitors with information that would enable them better target the larger CPs' customers.

It is unlikely that this competitive perspective will change, but there are increasing pressures, especially from new entrants to the consumer credit market, for freer access to data for marketing purposes. This issue could be resolved by putting power in the hands of the consumer rather than the bank to determine the use (and the users) of a consumer's data. The new 'Comprehensive Right' proposed by the Productivity Commission may become the facilitator for this. However, it should be noted that in an opt-in CCR regime, unrestricted access to the credit file for marketing purposes will lead to non-participation by larger players and, in a mandatory CCR regime, such a move would meet with strong resistance – expecting an organisation to take active steps to make it easier for new entrants to pick off their best customers is akin to 'asking turkeys to vote for Christmas'.

Either way, this is an arena where it behoves industry to take a proactive role in discussing and determining an industry code of conduct for such data uses as part of the broader industry-led framework recommended here and to engage with government and regulators through that process to inform and support the development of an effective overarching regulatory framework that is able to accommodate ongoing technological and industry innovation and evolution.



A BALANCE NEEDS TO BE DRAWN IN ENDEAVOURING TO ENSURE THAT ADEQUATE SERVICEABILITY ASSESSMENTS ARE CARRIED OUT IN SUPPORT OF RESPONSIBLE LENDING OBLIGATIONS VERSUS AVOIDING OVERLY INTRUSIVE FORAYS INTO THE APPLICANT'S PRIVATE LIFE



7. GOVERNANCE FRAMEWORK OPTIONS FOR FUTURE OPEN DATA SHARING

A new governance framework should seek to balance privacy concerns with economic and consumer benefit, adopting principles-based regulation and rely for operational purposes on a self-regulating code of conduct. The credit reporting arena provides a possible blueprint for this, comprising the overarching regulatory framework (Part IIIA of the Privacy Act), supported by a set of regulations (the Credit Reporting Code) and underpinned by a self-regulated industry 'code of conduct' (the Principles of Reciprocity and Data Exchange (PRDE)) and a common data standard (Australian Credit Reporting Data Standards (ACRDS)). Importantly, this framework limits the role of a regulator to ensuring regulatory compliance and leaves industry to work out and govern the myriad operational details and complexities and day-to-day intra-organisational commercial and conduct issues.

Commercial enterprises will act to maximise the generation of profit. Together with market demand for improved products and services, this drives innovation. Commercial interests and market forces will tend to push this envelope to the limits exerted by business case, technological capabilities, legal and ethical considerations and not all risks and issues are identifiable in advance. A pragmatic framework that includes regulatory and industry standards and codes of conduct and which allows for progress and experimentation while minimising down side risks is key.

Such a framework, with legislation and regulations underpinned by an industry self-regulated code of conduct is one option that would provide for a balanced outcome with inbuilt flexibility, recognising that the world of data sharing will evolve rapidly and at a pace much faster than legislation could ever match. Accordingly, it is essential that industry becomes engaged with the development of this framework as soon as possible, to ensure that practitioners' expertise is embedded within a "future-proofed" regime.

When contemplating regulatory oversight,

the question of "which regulator" is also an important consideration, with overseas practice demonstrating the benefit of oversight by an economic function such as ASIC, rather than by a Privacy function such as the OAIC. Either way, it is debateable whether an optimal balanced outcome would result should only one of these two alternative regulatory viewpoints have sole oversight over the data ecosystem. A regulator tasked with the protection of privacy is inherently at odds with the notion of optimising data utilisation in pursuit of economic gains. Similarly, an economically mandated regulator aiming to optimise economic productivity or minimise prudential risks, while not blind to these matters, will not be primarily concerned about privacy issues.

The inherent "tension" between these two objectives could act as a system of checks and balances ensuring that data access and utilisation is not overly restrictive nor overly permissive. That being said, having two different regulators with different core objectives overseeing the same system inevitably creates challenges for enterprises attempting to operate in compliance with potentially conflicting regulatory rules of conduct.

The option of a new 'Data Regulator' as proposed by the Productivity Commission Inquiry into Data Availability and Use could better address this need, provided its mandate was appropriately framed to ensure that a transparent and sustainable balance between consumer privacy and commercial productivity would be achieved²¹. Alternatively, the Privacy Principles and Act could be updated to ensure that the general rules and principles cover the intended use of this increased data asset with specific use cases being governed under which ever Regulator controls that specific industry and function.

²¹ <http://www.zdnet.com/article/economics-committee-denies-banks-data-sharing-responsibility/>



8. CONCLUSION: WHERE TO FROM HERE?

We are entering an era where the pace of technological and business change is running ahead of the regulatory and governance structures required to ensure that data sharing as a trusted activity contributes as fully as possible to commercial success, productivity and economic growth.

Absent a robust, secure governance framework for open data sharing – which goes far beyond the reach of the current Privacy Act – there is a very real danger that the potential of the “shared data economy” will not be realised and that a range of unfavourable unintended consequences may result. Without proper controls, security and transparency, acting with the consumer’s interests at heart, it will be very difficult to develop the trust required to fully unlock the benefits of data sharing.

The Productivity Commission has already set out along this path, recommending the creation of a new Data Sharing and Release Act, embedding a new Comprehensive Right for consumers. An industry response to inform policy and take a leadership role in the formulation of specific frameworks and standards governing and supporting more open data sharing is needed. ARCA is well placed to act as a conduit for industry views.

As this paper highlights, there are a number of complex issues and questions to be addressed. Not one of these questions is simple to answer and all deserve careful and urgent thought as to how best to address them. The principles and insights encapsulated in the credit reporting environment provide a solid foundation to work from, but do not present a fully-fledged answer to the entirety of the need.

A collective, industry-wide initiative aiming to address these topics, starting with a series of workshops, is needed to inform effective engagement with policy makers and support the development of a broader governance framework, including a self-regulating code of conduct, which represents the appropriate balance between consumer protections, privacy, and commercial and consumer benefit.



IT IS ESSENTIAL THAT INDUSTRY BECOMES ENGAGED WITH THE DEVELOPMENT OF THIS FRAMEWORK AS SOON AS POSSIBLE, TO ENSURE THAT PRACTITIONERS’ EXPERTISE IS EMBEDDED WITHIN A “FUTURE-PROOFED” REGIME

