Regulatory trends and emerging practices in access to customer data, portability and data sharing in the financial services sector

Paper for the *Banking & Financial Services Law Association Annual Conference*
31 August – 2 September 2017

Peter Leonard[1]
Principal, Data Synergies
Advisory Board Member, NSW Data Analytics Centre

1 Data: introduction and the big picture

Around the globe battles are now being fought over access to, and use of, consumer data.

Most wars are fought for control of assets that are scarce - water, food or land. Data is different: it is self-evident that data is now abundant. With advancements in technology, communication, storage and processing power, year on year the data captured increases in volume, type and applications. In 2018, it is estimated that we will globally generate 50,000gb of data *every second*. Such telephone book number may seem meaningless, but to put data generation into perspective, consider that in 1992 humans only generated 100gb of data *per day*. In 2007, Steve Jobs introduced the iPhone 1 with the catchphrase "this will change everything". Two years later, in 2009, the number of devices connected to the internet first exceeded the total world population. Add up all the accumulated data (knowledge and detritus) of human history and compare: 90% of the world's data has been created in just the last two years. And today 127 new devices, most communicating machine-to-machine (e.g. ATMs, merchant terminals, smart-everything IoT devices and so on), connect to the internet every second.

Most commentators, whether or not 'privacy advocates', agree that laws that give individuals transparency and a degree of control over how sensitive personal data about them is handled by others are essential for ensuring that people will be treated fairly in today's data-rich world. But some questions remain in high contention:

- Who should be entitled to capture the value of capture and transformations of data?
- Should control over uses of data extend to a right to share in value derived from that data? Is so, what's a fair share for consumers?
- Once we start to think about abstract concepts of 'data value' and 'fairness', how do we reconcile such abstractions with consumer protection laws, laws relating to intellectual property

[1] Peter Leonard is a data and technology business lawyer and consultant and principal of Data Synergies, a new data commercialisation consultancy. Peter was a founding partner of Gilbert + Tobin. Following his retirement as a G+T partner in 2017 he continues to assist G+T as a consultant. Peter chairs the Australian IoT (Internet of Things) Alliance's Data Access, Use and Privacy work stream and the Law Society of New South Wales Privacy and Communications Committee. The IoT Alliance is Australia's peak body bringing together industry, consumer organisations and governments to address issues affecting IoT adoption and implementation. He also participates in the Australian Computer Society's Data Taskforce and the ACS' Artificial Intelligence Ethics Committee.

and confidential information (trade secrets), and with privacy and data protection laws? In particular do we need to confer upon individuals new rights in data about them?

- How can we sensibly address sharing of data value, and questions of mandating sharing through new law or regulation, when we have little idea as to how data uses and applications will evolve over any period of time longer than, say, 24 months, or which entities will capture that value?

This paper will not attempt to answer each of these questions, for the obvious reason stated in the fourth question: even expert commentators differ as to how data uses and applications will evolve, and what value will be created and by whom, in the future. It is also fair to say that we are so early in thinking systematically about data value that questions such as these are seldom formulated and rigorously examined. Instead, many commentators as to the future data applications and futuretech jump straight to important, but less pressing, topics such as: *How do we program autonomous cars to deal with the trolley-car dilemma? How can we stop automated decision making from engaging in unacceptable discrimination? Are smart (blockchain enabled) smart contracts <u>really</u> that smart? How do you work out who is legally responsible for bad outcomes of machine learning applications? Must robots be ethical?* These are all important questions, but with all due respect to the growing army of authors that address such topics, they are not as 'here and now' as questions about consumer data.

This paper covers a broad territory. Keeping this paper to manageable length has necessitated simplifications and perhaps overly broad statements. This paper is not drafted as a learned legal treatise. Citations are made principally as a guide to further reading. Upon request the author would be happy to guide readers to other relevant papers by the author, and excellent materials published by other authors, that address relevant areas in greater detail.

2 Data and the financial services sector

Our focus in this paper is the financial services sector and (only) collection and use of customer data by financial service providers (**FSPs**) within that sector.

History tells us that technological innovation usually 'follows the money'. Not surprisingly, the banking sector has been an early adopter of new technologies that now enable a wide variety of electronic banking products. These technologies include ATMs, EFTPOS machines, online banking, data feeds to online accounting systems, systems for detection of fraudulent and suspicious transactions, debit cards, cardless tap-and-go, and so on.

The banking sector has been a somewhat slower adopter of data analytics fuelled consumer-facing products and services. This is not through shortage of available data. Data in the financial services sector is unusually 'rich', in the sense of being deep, diverse, and actually or potentially (through inference) descriptive of customer attributes, interests, preferences and behaviours. But FSPs also have a complex relationship with their customers as to customer data.

A few relevant propositions:

- Banks are custodians of money because customers trust them with their money. Consumer trust is hard won and easily lost. Customers won't forgive bad stewardship of data about them just because a bank doesn't lose their money. There is usually another bank ready to step in and take the customer.

- The financial cost of bad stewardship of data continues to rise. Just ask Ashley Madison.

- Much data is collected by FSPs as a necessarily incident of the customer transacting through the FSP. Taking banks as an example, this data includes both customer volunteered data required for loan assessments and observed transactional data collected by a bank in relation to its customers and others through electronic payments, salary payments, lending credit and debit card issuance and acceptance and merchant transactions. Customer transaction data is not volunteered by the customer, or collected through customer initiation by the customer of provision of data, as distinct from the conduct of a transaction. It is not a 'free gift' – as we will

see in section 3 of this paper, the cost of its collection and collation is substantial – but the fact that collecting and collating this data is substantial does not alter the fact that this data is not volunteered. 'Consent' as to uses of non-volunteered data is inherently problematic in circumstances where all FSPs similarly require the right to make relevant uses of that data.

- Some rich data is collected by FSPs through customer initiation of provision of data in applications for credit cards, loans and mortgages. Many customers would not consider this data 'volunteered'. Contrast the willingness of many consumers to volunteer data in the course of interactions with social networking sites and many online service providers.

- Banks deal with a 'broad church' of customers, who exhibit widely different perspectives and views as to privacy and fairness, and appreciation and appetite for risk.

- Most customers don't understand how data may be used, and how to evaluate what is fair and reasonable and what is not. This position will not change quickly. Bad actions by bad actors may hold back changes in perceptions of customers. Many data-driven applications are complex to explain and when explained sound frankly spooky, even when those applications are provided from properly privacy protective and legally compliant data environments.

- Discussions in the community as to social licence for expanded uses of data are nascent and often ill-informed – although note the admirable social engagements initiatives of New Zealand's Data Futures Partnership.[2] Discussions as to social licence in Australia have also not been assisted by a number of high profile data mishaps over 2016-17 by various Australian Federal public sector agencies.[3]

Having regard to these propositions, it is perhaps not surprising that banks have been a slower provider of data-driven, analytics-based consumer products and services.

Is that rate of adoption about to radically change?

Let us consider further the nature of data.

3 Is data the new oil for FSPs? The data value creation process

It is often fairly said that data is 'the new oil'. However, this catchy epithet is misleading. The methods to value physical commodities such as oil do not capture some unique qualities of data. Unlike physical commodities, data can be reused, is not scarce, cannot of itself be controlled and monopolized by a small number of owners, and has little inherent value.

Data derives value to the extent that a data custodian has both technical capability and legal right to:

- to capture data points of sufficient granularity and number in a readily usable form, and

- to bring together that data, and

- to transform and then analyse the data, to derive meaningful insights and to enable actionable decisions to be made by the data custodian (or by another person with whom the custodian shares the information).

[2] See the Data Futures Partnership material available through http://datafutures.co.nz/our-work-2/talking-to-new-zealanders/social-licence/ and https://trusteddata.co.nz/ and in particular Exploring Social Licence - A conversation with New Zealanders about data sharing and use, July 2016, and *A Path to Social Licence: Guidelines for Trusted Data Use*, August 2017.

[3] See further Peter Leonard, *Emerging Concerns for Responsible Data Analytics: Trust, Fairness, Transparency and Discrimination*, Paper for the NSW Data Analytics Centre Showcase, 12 July 2017. Many media reports have chronicled the string of privacy related concerns arising as to uses of data by Australian government agencies over the 2016-17 Australian financial year. By way of example, see articles in *The Mandarin* including Matthew Beard, 6 March 2017, 'When it comes to trust, a good offence is your worst defence' http://www.themandarin.com.au/76454-high-price-to-pay-to-correct-the-public-record/ and Anna Johnston, 30 June 2017, 'A litany of privacy disasters: how to ruin public faith in just 12 months' http://www.themandarin.com.au/80791-litany-privacy-disasters-ruin-public-faith-just-12-months/.

The first value add in the data value creation process is data capture in a form that enables aggregation of granular data points.

Capture and aggregation may be an inherent aspect of delivery of a service, or a by-product of delivery of a service (a fortuitous yield of useful information). Often the value of particular data is not readily apparent when first collected. So nowadays, with low cost of data capture, communication and storage, most data custodians 'over-collect', warehousing 'raw' information unanalysed and sometimes not fully aggregated or transformed.

The second value add is data normalisation and cleansing and transformation.

Transformation of disparate data points and data fields to make them useable requires a data custodian to incur significant upfront development and implementation costs. Development of reliable processes for data cleansing and normalisation is time consuming and expensive, particularly where input data has been captured in multiple or legacy systems. For most data custodians, systematising the various data transformations that are required in order to create reliably consistent data fields for merging and aggregation of data sets is a significant episodic cost of doing business. For many, this activity remains a substantial costs centre. It is accordingly a barrier to data analytics at scale.

Once data is transformed to be capable of reliable application and use, a data custodian has useful transaction data. Relatively straightforward value add enables presentation of data in the form of account statements, reports, segmented activity reports, and so on. More complex value adds may be required to present that information in a standardised format to a customer dashboard or other portal or to an external data feed (e.g. NAB's electronic feed to XERO). For most data, this is the end of the data value creation journey that began with raw disaggregated observed data and volunteered data about a transactor (identifiable individual or an account or a device) and passes up to transformation and aggregation and further up to transaction reporting and billing.

Data science adds new tiers of data value creation. Where data analytics is to be conducted on data about human transactions, the pathway may be either of the following.

- Consent-based use through analysis of data about individuals that are re-identifiable from the data itself or by reference to other available information. In many jurisdictions (including Australia and New Zealand) this is regulated as a use or disclosure of 'personal information' (in some other jurisdictions referred to as 'personal data' or 'personally identifying information' (**PII**))[4]. Note that this use and subsequent disclosures of outputs by banks must also comply with the rule in *Tournier's* case.[5]

- Use through analysis of data about individuals that has been pervasively de-identified through substitution of transactor keys for personal identifiers or using other deidentification methods. Where deidentification and accompanying safeguards are such that the risk of reidentification of individuals is remote, the now more commonly accepted view is that such use is not a use of personal information. However, the act of deidentification may itself be a use of personal information, and subsequent disclosure of facially deidentified data may be a disclosure of personal information if the information as released is available to any entity that could re-identify individuals within the relevant data set or by reference to other information reasonably available to that entity.[6]

The first step to realising the third value add is data discovery. Once data is transformed, 'discovery' can be undertaken using trial data and trial code to find correlations between data attributes, including through use of machine learning to refine attribute correlation. This is the most uncertain and highest value area of data science, requiring creativity and close teamwork between business analysts, 'quants', code developers and consultants and data visualisation experts. There remain shortages of

[4] See for example Office of the Australian Information Commissioner, *What is personal information?*, May 2017 https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information; *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017) per Kenny and Edelman JJ.

[5] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461

[6] See further Peter Leonard, *Emerging Concerns for Responsible Data Analytics: Trust, Fairness, Transparency and Discrimination*, Paper for the NSW Data Analytics Centre Showcase, 12 July 2017.

experienced personnel in these areas. Accordingly, this phase is both skilled labour intensive and expensive.

The next step is the development phase: if and when useful (statistically reliable, relevant and meaningful) correlations are found, production code can then be developed, trialled and then applied to 'real' transaction data in a production environment.

Finally, the application phase: generation of outcomes and insights can be applied in a business. Sometimes these outcomes and insights enable new businesses: Google's search business and Facebook's social networking generates insights that informs their respective paid advertising businesses, and development of new adjacencies such as secure messaging, artificial intelligence supported search and so on. The value of these insights also create novel market structures. The two-sided nature of search and social networking enables those services to be provided for free to users that are then funded through sale of advertising and monetarisation of insights about those users. Clearly, this user data is very valuable.

To summarise the current state of data science as applied to customer data:

- The value of data is derived through increased availability of data capable of aggregation and merger with other data sets to provide information in a form readily assimilated and used by humans (such as visualisations and other value-added presentations).

- Through data analytics methods of increasing sophistication, data acquires additional value. For example, algorithmically generated customer segmentation analyses and tools enable service providers to improve their ability to define and then target increasingly granular customer segments and to differentiate as to price and other terms offered to those customer segments.

- Data is also more readily available for analysis because it is more 'discoverable' as data taxonomies are standardised and as data extraction tools refined. There is more data that can be discovered and used. There is a rapidly expanding better range of already developed and tested data analytics tools and methods.

- Data is more readily available because businesses interact with each other and with consumers through increasing flows of consumer data and because each businesses is increasingly algorithmically driven in its own operations (therefore requiring better integration and availability of data across the business).

- Data value can be realised through improved ability of business to understand characteristics (attributes, preferences and interests, inter-relationships) of their customers and to infer characteristics of 'lookalike audiences' of prospective customers.

- Tools and methods for analysis and presentation of actionable insights are now widely readily available, including powerful tools readily available to consumers in the form of apps on smart phones or access to service comparison engines.

4 Data sharing – further value creation, or value destruction, for financial services providers?

A data custodian may derive further data value through sharing with third parties either data itself, or insights derived through transformation and analysis of data. The term 'data sharing' is often used indiscriminately to describe any of:

- provision of deeper and richer data to customers,

- sharing of data provision of data as a necessary incident of provision of particular services (e.g. credit card acceptance or payments facilitated through third party payment services providers),

- sharing (pooling) of transactional data sets,

- sharing of insights derived from analysis of data, and

- data linkage projects where attributes are joined in a privacy protective environments where the transacting individuals that have such attributes are not identifiable.

Sometimes 'data sharing' is used to describe only a non-mandated provision of data or a transactional relationship where data sets are joined or pooled in some way. There is no commonly accepting definition of data sharing. Many discussions as to 'data sharing' are hampered by lack of mutual understanding of discussants as to what 'data' is actually being shared (and whether what is shared is data or derivations from data such as insights), with whom, and as to the relevance of controls which limit which entities can see particular information and then under what conditions.

Data sharing may be:

- restricted by contract or by operation of laws, such as privacy and data protection laws, consumer and competition laws and duties of confidentiality such as the *Rule in Tournier's Case*, or

- required by law or regulation, such as mandatory reporting under AML/CTF laws and proposed comprehensive credit reporting.

The recipient of data sharing might be any of:

- the person to whom the data relates (the 'data subject'),

- a third party data analytics services provider to the data custodian,

- a third party provider of data commercialisation services, such as an ad exchange,

- an agent for the data subject. This agent might be (1) a data subject-enabled price or product comparison engine or (and that engine's 'application program interfaces (**APIs**), 'bots' and 'screen scrapers') or (2) a user of a data feed such as accounting services such as XERO, MYOB and Quicken, and so on,

- a new service provider competitive with the data custodian. That new service provider (or its agent) may access customer data either (1) by access to open or partially open data sets within the data custodian's data, through data custodian-facilitated use of application programming interfaces (APIs may be any of data custodian defined, industry defined or regulator mandated), or (2) through facilitation of the data subject, such as through the data subject handing over pins or passwords to enable the service provider to use bots or otherwise 'screen scrape' data from the data custodian's online customer portal).

Many fintechs have business models based upon a customer empowering the fintech to draw and use data from an incumbent provider of financial services to that customer. Some fintechs have business models that leverage other data sources in order to power offer or provision of a different suite of products or services.

Consider a new examples.

Technology companies are already in facilitating switching decisions across a broad range of industry sectors. Data aggregator Envestnet Yodlee acts as intermediary between the banks and start-ups, pulling data from U.S. banks and translating the data into a form that start-ups like Betterment, Mint and Digit can use. Technology companies like Mint and Betterment provide services that let people link all their various bank-account and credit-card information. The consumer benefit is to make budgeting and bookkeeping easier. The business case is targeted offer (with targeting based upon analysis of the customer data) of new kinds of loans and investment products to consumers. A response by some banks has been to restrict the sharing of this kind of data with technology companies, including by refusing to pass along information such as fees and interest rates they charge. Some banks say they want to give people access to data about them, but they want security

controls and authentication standards and agree restrictions as to how intermediaries request and handle this data.

Rakuten Ichiba is Japan's single largest online retail marketplace. Rakuten Ichiba also provides loyalty points and e-money usable at hundreds of thousands of stores, virtual and real. It issues credit cards to tens of millions of members. It offers financial products and services that range from mortgages to securities brokerage. And the company runs one of Japan's largest online travel portals and instant-messaging app, Viber, which has some 800 million users worldwide. Is Rakuten Ichiba a retailer? A financial services provider? It is both, and more.

In China large technology companies like Ant Financial and Tencent have emerged as leading providers of a range of financial services, in a departure from the bank-led model in the US and Europe.

The World Economic Forum (**WEF**) in an August 2017 report[7] has identified the emergence of distinct financial systems in China, Europe and the US. The report concludes that while fintech companies have "materially changed the basis of competition" in financial services, they have not yet materially changed the competitive landscape itself. Fintech businesses have pushed the pace and direction of innovation, but "have struggled to overcome the scale advantages of large financial institutions". The report suggests that customers have been less willing to switch away from incumbents than expected and that new innovations have not been enough to encourage them to do so. The smaller companies have also struggled to create the infrastructure they need and to establish new financial services ecosystems, such as alternative payment rails or alternative capital markets. "They have been much more successful in making improvements within traditional ecosystems and infrastructure."

The WEF report also contends that Amazon and Google have had a bigger impact on the development of banking systems than fintech start-ups. The WEF report notes that this situation creates risks for both incumbent financial services providers and fintechs. "Many financial services companies are turning to large technology firms like Amazon, Google and Facebook to provide functions including cloud computing, customer-facing artificial intelligence and customer analytics. While this can accelerate innovation, it would also create a risk if these technology companies decide to enter the financial services industry themselves."

5 Key strategic data decisions for financial services providers

As new hybrid competitors and intermediaries emerge, every financial services provider will need to make, and regularly review, a number of the key strategic decisions:

- *To what extent should the financial service provider share the value that the provider can derive through data, by empowering the provider's customers to make better, more informed decisions and meeting demands by customers for enhanced access to data to facilitate customers analysing that data themselves?*

- *Should a provider respond only to regulatory compulsion, or should a provider strive to differentiate itself from its competitors by addressing demand by (some) customers for greater access to, and control over, financial data about them?*

- *Is it viable to keep customer data within a provider-controlled data ecosystem? To what extent will customer demand or regulatory intervention be such that certain customer data should be proactively made available into a more open data environment? If so, how much data, how made available, and to whom?*

- *How does a provider make data more available while adequately protecting its customers from security risks? In what circumstances should customers be taken to know and assume the consequences of such risks? More specifically, how does a provider verify that a customer properly understands the risks of conferring agency upon an intermediary to conveniently*

[7] World Economic Forum, *Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services, Future of Financial Services series*, August 2017.

access sensitive financial data about a customer? How does a provider verify that an intermediary (such as a price comparison engine) purportedly authorised by a customer to access certain sensitive financial data about that customer is so authorised and will handle that data with due care?

Frequently discussions as to open data in the financial services sector talk about customer access to 'their data'. When considering possible regulatory interventions to mandate access to customer data by customers or their agents, threshold questions for financial service providers should be:

- Who owns which data sets?
- Do rights of ownership or control of data impede a regulator from requiring these data sets to be opened to fintechs, competitors, customers or their agents?

The next sections of this paper address those questions.

6 What is 'customer information'?

'Customer information' and 'customer data' are inherently ambiguous terms that may lead to incorrect assumptions or conclusions that:

- a customer owns relevant information,
- a customer should be entitled to access relevant information, or
- relevant information may not be substantially value-added (whether through the bank expending efforts and incurring substantial costs in capture and classification of this information, or through the smarts, effort and expense of subsequent analytics).

The term 'customer information' is commonly used to refer to any and all of:

- basic contact details about a customer (usually information volunteered by a customer),
- value added details about a customer that are CRM (customer relationship management) and not directly financial or financial transactional in nature (i.e. employment details, related accounts, age, names of spouse and siblings, etc.),
- account statements and transactional records,
- value added presentations or analyses of a customer's transactions,
- value added financial information that are factual in nature such as credit assessments and credit reports, and/or
- data analytics outputs such as features, attributes or modelled scores as applied to an particular customer and associated with that customer in any bank record (imputed or inferred data).

There is not a generally accepted view as to the distinction between data and information. Nor is there a generally accepted view as to the distinction between raw data and value added data.

Use of the term data may lead to inferences that it is 'unprocessed' or 'not analysed' and therefore not of significant commercial value. As we have already noted, the capture and transformation (through cleaning and verification) of data to be ready for analytics will often be a substantial cost component of information management within an FSP's operations and of any complex data analytics project. A commonly stated rough rule of thumb is the cost of data analytics projects is 75% data normalisation, cleaning and transformation and 25% data analytics.

Within the data sets and data fields comprising financial services information about customers is a subset of personal information about (identifiable) individuals that is relevantly subject to, (in Australia) the (Federal) *Privacy Act* 1988 (C'th) and (in New Zealand) the *Privacy Act* 1993.

These Privacy Acts creates a limited set of statutory rights exercisable by an affected individual (and Privacy Commissioners in relation to contraventions of these rights) in relation to a collection, use or disclosure of personal information about an individual - specifically:

- **transparency/right to know**: to know how personal information about them is collected, used or disclosed (at least in circumstances where the individual is reasonably identifiable by reference to that information alone or in conjunction with other information available to any entity holding that information);

- **control**: to control how this personal information about them is collected, used or disclosed.

The right of access to personal information is exercisable against whatever entity holds personal information about an individual and accordingly is not affected by corporate structuring or sub-contracting.

The right of transparency, and the absence of any proprietary right of an individual in information about them, are now commonly understood. However, there is significant debate as to the scope of the right of 'control'. In Australia and New Zealand, it includes a right of individuals to access personal information (Australia: '*if it is reasonable and practicable to do so*', New Zealand: '*if the information requested is …readily retrievable*'), to require correction of incorrect details, and to require deletion or destruction of personal information. The organisation responding to the right of access may determine the form in which access is made available and accordingly may present extracts or reports of the information. The right of access does not include any right of a data subject to require a data custodian to provide electronic data in a form which would facilitate an individual enabling an agent to receive and use that personal information. That noted, In Australia the data custodian must give access to the information in the manner requested by the individual if it is reasonable and practicable to do so and must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

Australian or New Zealand privacy laws do not affect in any way:

- characterisation of whether there are proprietary interests (i.e. in copyright) in personal information about an individual within the database,

- characterisation of which data sets and data fields comprising bank information about a customer are subject to the bank's duty of confidentiality, or

- determination of which data sets and data fields are commercial-in-confidence to the bank and at what point in transformation or limited disclosure of that data (i.e. to a customer in response to a customer's online enquiry) this data ceases to be commercial-in-confidence.

7 Ownership of data: copyright in databases of bank information about customers

So if a FSP's customer does not own the FSP's information about them, does the FSP? Many commentators wrongly assume that copyright protects databases. However, this copyright protection is quite limited, particularly in Australia. The Australian case law relevant to copyright in compilations and databases and computer-generated works, and in particular the two leading cases (the decision of the High Court of Australia in *IceTV Pty Ltd v Nine Network Australia Pty Ltd*[8] and the subsequent decision of the Full Federal Court in *Telstra Corporation Limited v Phone Directories Company Pty Ltd*[9], create significant barriers impeding successful claims for copyright in data.[10]

[8] *IceTV Pty Ltd v Nine Network Australia Pty Ltd* [2009] HCA 14

[9] *Telstra Corporation v Phone Directories Company* [2010] FCAFC 149

[10] Fitzgerald, Anne M. & Dwyer, Natasha, *Copyright in databases in Australia* at https://eprints.qut.edu.au/50425/. See also *JR Consulting & Drafting Pty Limited v Cummings* [2016] FCAFC 20.

Copyright is a bundle of intangible rights created and defined by law in relation to subject matter that is within the classes of creations of intellectual endeavour of human 'authors' as recognised by the *Copyright Act* 1968. The classes of copyright subject-matter are the original expression of literary, musical, artistic and dramatic works, as well as their industrial form, such as books, computer programs, sound recordings, films and broadcasts.

The subject matter of copyright within the classes recognised by the Copyright Act 1968 are a species of property within the genus 'personal property', which encompasses tangible or 'corporeal' things and certain intangible or 'incorporeal' legal rights. Tangible things exist independently of law: the law governs rights of ownership and possession in them, including whether they can be 'owned' at all. Intangible property includes choses in action and rights in copyright and other intellectual property rights, shares in a corporation, beneficial rights in trust property, rights in superannuation and some contractual rights, including, for example, many debts. Intangible rights are created by law. Intangible property exists only because of law, but once recognised by law intangible property is entitled to the general protections afforded to property under Australian and New Zealand law, including against misappropriation[11], and in Australia to the constitutional protection against acquisition other than on just terms.[12]

Electronic data of itself is no more than a collection of information. Broadly, what may be recognised and protected as copyright subject matter (a 'literary work') is the fruit of intellectual endeavour of humans in selecting, structuring or organising data/information into a database, not the underlying data. It is strongly arguable that by selection and structuring and organising electronic data into a database, and subject to identifying human authors of the selection, structure and organisation and sufficient originality in that selection, structure and organisation, information as selected, structured or organised in a database may qualify for copyright protection. However, on the current state of Australian case law as to copyright in databases, such cases will be unusual and difficult to establish. Generally, only a sufficiently novel and substantial form of presentation of outputs from enquires on a database, and the software that is used to manage the data and generate reports and other outputs from that database, will qualify as copyright subject matter protected by copyright.

It is not generally relevant to copyright law whether substantial expense has been incurred or effort expended by a business in collecting and inputting data into a database, in cleansing or otherwise transforming data and making it ready for use or analytics, in operating the data processing environment, or even in creating data cubes by algorithmic analytics that classifies data by some organising attribute. What is relevant to determination of whether copyright subject matter exists is whether it is possible to identify a non-transient work that is the output from application of a level of intellectual endeavour that gets over the low bar of 'originality' of an identifiable group of humans employed by that business (or of contactors that assign copyright to that business), in selecting, structuring and organising that information as presented in that non-transient work.

Of course, data may be transformed so that it becomes protected. Just as an author selects words from the English language and structures and organises those words into a grammatical form that is a protected literary work, data may be transformed into a literary work. But while the data is at rest in a database, albeit classified by data fields or by other attributes, the data itself is generally not protected by copyright. By contrast, it is the presentation of that data expressing the intellectual endeavour of identifiable humans in applying those attributes to present that data in a particular 'original' form of expression that can be protected copyright subject matter.

[11] But see Kelly McFadzien and Tim Sherman, 'Digital files as property: a curious case in New Zealand' *Privacy Law Bulletin* April 2016, pp71-73.

[12] Section 51(xxxi) of the Constitution provides that the Commonwealth Parliament may make laws with respect to "the acquisition of property on just terms from any State or person for any purpose in respect of which the Parliament has power to make laws". The High Court has taken a wide view of the concept of 'property' in interpreting s 51(xxxi) of the Constitution, reading it as 'a general term': '[i]t means any tangible or intangible thing which the law protects under the name of property'. A chose in action may be property: a statute extinguishing a vested cause of action or right to sue the Commonwealth at common law for workplace injuries was treated as an acquisition of 'property' in *Georgiadis v AOTC* (as the claimant was effectively stripped of all of the rights of an 'owner' of a chose in action exercisable against the Commonwealth) *Georgiadis v AOTC* (1994) 179 CLR 297. But see also *JT International SA v Commonwealth* (2012) 250 CLR 1 concerning the Tobacco Plain Packaging Act 2011 (Cth).

It follows that the mere fact that data in a database has been transformed through data analytics does not of itself qualify the data as so transformed for copyright protection. The transformation may change the character of the data by appending attributes or metadata that qualify the database for copyright protection. However, if the 'underlying data' is then shorn of the attributes or metadata, that underlying data reverts to its native state and is not of itself protected by copyright (although as we note in the following sections, it may well be protected as 'trade secret' or 'confidential' information).

In summary, data as accessible through a database generally will not be copyright subject-matter, notwithstanding that very substantial expense may have been incurred in capturing, cleansing and curating that data and notwithstanding that this database may be a significant intangible asset of a business and strenuously protected by that business as confidential information (trade secret).

8 *Tournier's case and equitable duties*

As most readers will be aware, the basic rights and obligations of a bank to its customers are defined by contract. In general terms, a banker-customer relationship is traditionally expressed as a 'debtor-creditor' relationship: the bank accepts deposits from its customer and becomes the customer's debtor, the bank lends money to customers and becomes the customer's creditor. The contract is comprised of both express terms and terms implied by the courts. The most famous implied term is the contractual duty of confidence as articulated by Bankes LJ in *Tournier's case*.[13] In accordance with that decision, it is an implied term of the contract between a banker and a customer that the banker will keep the customer's information confidential. This duty is subject to a number of qualifications. Bankes LJ classified these qualifications under four headings (at 472):

> "(a) where disclosure is under compulsion of law; (b) where there is a duty to the public to disclose; (c) where the interests of the bank require disclosure; (d) where the disclosure is made by the express or implied consent of the customer".

In addition, the banker-customer relationship contractual relationship is overlaid by equitable principles, operation of many statutes, including consumer protection legislation and the *Privacy Act* 1988 (C'th), the Banking Industry Code of Practice and tort law.

The banker-customer relationship is not one of the accepted fiduciary relationships[14] and the contractual duty of a banker to a customer is not of itself a fiduciary duty, except in special circumstances.[15] It follows that as a general principle and in the usual course the bank is entitled to prefer its own interests to those of the customer, unlike a trustee or a professional such as a doctor or lawyer. That noted, the courts will in certain circumstances find equitable obligations owed by banks to customers in relation to particular activities or practices.[16]

In some jurisdictions the characterisation of fiduciary relationship has been considered relevant and possibly decisive as to rights of the person to whom that obligation is owed to access certain information about them from records held by the fiduciary.[17] That is not the position in Australia. The High Court of Australia held that no right arose in Australia in the case of the clear fiduciary relationship between a doctor and patient, in respect of medical notes as taken by a doctor. As stated by Brennan CJ in *Breen v Williams*[18] (often referred to as *the Medical Records Access case*):

---

[13] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461. As to other implied terms, see Atkin LJ in N *Joachimson v Swiss Bank Corp* [1921] 3 KB 110 at 127, cited with approval in *Tournier's case* by Bankes LJ.

[14] *Golby v Commonwealth Bank of Australia* (1999) 72 FCR 134 at 136.

[15] *James v Australia and New Zealand Banking Group Ltd* (1986) 64 ALJR 347, 391; *Commonwealth Bank v Finding* [2001] 1 QdR 168; *ACCC v Oceana Commercial Pty Ltd* [2003] FCA 156; *Timms v Commonwealth Bank of Australia* [2004] NSWSC 76. See further the discussion in Andrew Tuch, 'Investment Banks as Fiduciaries: Implications for Conflict of Interest' (2005) *MULR* 478 at 'Part II Theoretical Basis' pp481-484.

[16] See for example the cases discussed in John Glover, Banks and Fiduciary Relationships (1995) 7/1 *Bond Law Review* at 50.

[17] See for example the Supreme Court of Canada in McInerney v MacDonald (1992) 93 DLR (4th) 415 at 423. The *ratio* for the decision is limited and the reasoning in that case persuasively criticised by Gaudron and McHugh JJ in Breen and Williams at [34] –[42]

[18] [1996] HCA 57; (1996) 186 CLR 71 (6 September 1996). See also *Primary Health Care Limited v Commissioner of Taxation* [2010] FCA 419 and Judith Mair, *Who owns the information in a medical record? Copyright issues*, Health Information Management Journal 40/3 2001 at pp31-37.

> "If the approach is that a right to access and to copy arises because the information contained in the records is proprietary in nature, the approach mistakes the sense in which information is described as property. The sense in which information is so described was stated by Lord Upjohn in *Phipps v Boardman*[19] in these terms:
>
> > "In general, information is not property at all. It is normally open to all who have eyes to read and ears to hear. The true test is to determine in what circumstances the information has been acquired. If it has been acquired in such circumstances that it would be a breach of confidence to disclose it to another then courts of equity will restrain the recipient from communicating it to another. In such cases such confidential information is often and for many years has been described as the property of the donor, the books of authority are full of such references; knowledge of secret processes, "know-how", confidential information as to the prospects of a company or of someone's intention or the expected results of some horse race based on stable or other confidential information. But in the end the real truth is that it is not property in any normal sense but equity will restrain its transmission to another if in breach of some confidential relationship."
>
> As information is not property except in the sense stated by Lord Upjohn, the remedies which equity grants to protect against the disclosure of certain kinds of information do not have their source in notions of property. Deane J pointed this out in *Moorgate Tobacco Co Ltd v Philip Morris Ltd (No 2)*:
>
> > "Like most heads of exclusive equitable jurisdiction, its rational basis does not lie in proprietary right. It lies in the notion of an obligation of conscience arising from the circumstances in or through which the information was communicated or obtained."[20]
>
> Equity might restrain the respondent from disclosing without authority any information about the appellant and her medical condition that is contained in the respondent's records and, in that sense, it might be arguable that that information is the property of the appellant. Even if such a description were correct - and it is not necessary to consider that question - the description would provide no foundation for the existence of a right to access and to copy enforceable in equity. The mere possession by the respondent of his records relating to the appellant breaches no obligation of conscience and thus it attracts no equitable remedy that might clothe the information with some relevant proprietary character. There is no obligation in conscience requiring the respondent to open his records to inspection and copying by the appellant. Whichever approach is taken to the relevance of the law of property, it fails to provide any basis for the appellant's claim."[21]

Gummow J relevantly held that:

> "it could not be said that implication of a contractual term which entitled Ms Breen to examine medical records and obtain copies was necessary for the reasonable or effective operation of the contract between Ms Breen and Dr Williams"[22], and
>
> "to show a doctor owes a fiduciary duty in certain circumstances to a patient does not demonstrate a right in the patient to inspect and take copies of the notes and records of the medical practitioner".[23]

There therefore appears to be no basis to imply a contractual term into the contract between banker and customer to entitle a customer to access data held by the bank including transaction records, at least where transaction records are made available by a bank so as to enable the customer to deal with the bank in the normal course. Although the categories of equitable obligations of the bank to its

[19] [1966] UKHL 2

[20] [1984] HCA 73; (1984) 156 CLR 414 at 438

[21] Brennan CJ at [11] –[13]

[22] Gummow J at [29]-[30]

[23] Gummow J at [74]-[76]

customer are not closed and may include certain obligations of disclosure, there does not appear to be a basis to suggest that those obligations include an obligation to make available data held by the bank including transaction records, at least where transaction records are made available so as to enable the customer to deal with the bank in the normal course.

9 Protection as confidential information of databases of bank information about customers

So can a financial service provider assert that non-public information that the provider collates and holds about its customers, the customers' transactions and their attributes, is valuable confidential information that cannot be required to be disclosed without violating their rights in and to their confidential information? To answer this question, we need to consider the necessary character of confidence that gives right to the right to protect confidential information through an action for breach of confidence, and the nature of that right.

The accepted approach in Australia and New Zealand to an action for breach of confidence is to determine whether:

- the information is confidential,
- the information was imparted in circumstances importing an obligation of confidence, and
- there has been an unauthorised use or threatened use of the information.

Although all of the elements of the test must be satisfied, these elements are not in all cases completely independent of one another. For example, the circumstances in which the information is communicated may themselves dictate the confidentiality of the information in question.

In the High Court of Australia, the dissenting judgement of Gummow J in *Corrs Pavey Whiting & Byrne v Collector of Customs* summarised the relevant law and proposed additional elements to the test:

> "It is now well settled that in order to make out a case for protection in equity of allegedly confidential information, a plaintiff must satisfy certain criteria. The plaintiff: (i) must be able to identify with specificity, and not merely in global terms, that which is said to be the information in question; and must also be able to show that (ii) the information has the necessary quality of confidence (and is not for example, common or public knowledge); (iii) the information was received by the defendant in such circumstances as to import an obligation of confidence; and (iv) there is actual or threatened misuse of the information. … It may also be necessary… that unauthorised use would be to the detriment of the plaintiff."[24]

Notwithstanding this judgement being a dissent, the judgment has thereafter been applied and accepted in Australia as defining the elements of a breach of confidence action.[25]

Equitable doctrines in relation to confidential information have been developed to protect information that is commercially valuable and confidential (trade secret), but which does not fall within accepted species of property. As Gummow J stated in *Yanner v Eaton*:

> "Equity brings particular sophistications to the subject. The degree of protection afforded by equity to confidential information makes it appropriate to describe it as having a proprietary character, but that is not because property is the basis upon which protection is given; rather this is because of the effect of that protection."[26]

---

[24] *Corrs Pavey Whiting & Byrne v Collector of Customs (Vic)* (1987) 74 ALR 428 at paragraph 437. See also *Moorgate Tobacco Co Ltd v Philip Morris (No 2)* (1984) 156 CLR 414 at 438 (Deane J); 59 ALJR 77; 56 ALR 193. Fort New Zealand, see Kelly McFadzien and Tim Sherman, 'Digital files as property: a curious case in New Zealand', *Privacy Law Bulletin* April 2016 at 71-73 and *Dixon v R* [2015] NZSC 147; *Farah Constructions Pty Ltd v Say-Dee* (2007) 236 ALR 209, [2007] HCA 22; *Oxford v Moss* (1979) 68 Cr App Rep 183.

[25] See for example *Rapid Metal Developments (Australia) Pty Ltd v Anderson Formrite Pty Ltd* [2005] WASC 255; *Ekaton Corporation Pty Ltd v Chapman* [2010] SADC 150 per Brebner J at paragraph 17.

[26] *Yanner v Eaton* (1999) 201 CLR 351 at 388–9

Accordingly, we now talk about trade secret information being 'protected' by 'the law of confidential information' within the class of 'intellectual property', when in fact:

- there is no such law (instead there are equitable doctrines 'fastening on the conscience of the wrongdoer'),
- the subject matter is not 'property' as traditionally understood under Australian law, and
- the protection is not of the subject matter itself, but rather against the inequity of the wrongdoer deriving any benefit or advantage from that that they knew, or should have known, that they should not have.

A database to be protectable as confidential information must have the necessary quality of confidence. This involves objective and subjective elements. A subjective element is whether preservation of the confidentiality of the information is of substantial concern to the plaintiff. This can be established to adducing evidence demonstrating efforts that courts of equity expect a plaintiff to have taken to preserve the confidentiality of the information that the plaintiff claims is a valuable trade secret. An objective element is that the information must be of a kind that warrants protection.

If data has become part of the public domain, the data then is not confidential to the plaintiff and is no longer trade secret, however much the plaintiff considers this data to be valuable and confidential. However, some data (colloquially, 'slivers' of data) from a much larger collation of data may be put into the public domain, or more extensive data sets or fields may have circulation within a controlled and limited section of the public under legally binding conditions as to confidentiality, and the aggregation of data that comprises the database nonetheless retain the necessary character of confidence. Accordingly, an accessible database may be protected if the access is controlled and limited such that the combined accesses do not have the character of making the database broadly available. The way in which elements of the database are structured, aggregated, combined or used, and metadata fields, will generally also be protectable where these have the necessary character of confidence.

Because confidential information is only recognised in doctrines of equity as 'quasi-property', the originator or creator of the information can only in a loose sense be described as 'the owner'. However, although confidential information which is protected by an equitable claim of breach of confidence is not 'property', confidential information can dealt with (although arguably such dealings are not truly assignments or licences).[27] An 'assignee' or 'licensee' of confidential information can sue others for breach of confidence.[28] Databases are today traded for large sums even where due to absence of structure or organisation or transformation of data within the database, the database so traded probably does not (on current Australian copyright law) qualify for copyright protection. As already noted, data is not of itself protected by law, regardless of the size of the database and the expense of accumulating and capturing that data into a database. Effectively what is traded is the prospective chose in action that is an action for breach of confidential information action that equity confers upon persons or entities that control confidential information for so long as the relevant database retains the necessary quality of confidence.

10 New concepts: data portability and payments initiatives in the European Union and the U.S. Dodd Frank reforms

We have already noted that the right of access afforded to data subjects under Australian and New Zealand privacy laws does not include any right of a data subject to require a data custodian to provide electronic data in a form which would facilitate an individual themselves using that personal information or enabling an agent to receive and use that personal information.

In the European Union, the new right to data portability provided by Article 20 of the General Data Protection Regulation[29] (**GDPR**) will (from 25 May 2018) allows for data subjects to receive personal

[27] *TS & B Retail Systems Pty Ltd v 3 Fold Resources Pty Ltd (No 3)* (2007) 72 IPR 492 at 505-511 (Finklestein J*); Mid-City Skin Care & Laser Centre Pty Ltd v Zahedi-Anarak* (2006) 67 NSWLR 569 at 609-622 (Campbell J), *Douglas v Hello! Ltd* [2008] 1 AC 1

[28] *Douglas v Hello! Ltd* [2008] 1 AC 1

[29] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit this data to another data controller. The primary stated purpose of this new right is to empower the individual that is the data subject and give him or her more control over personal data.

Although the GDPR itself incidentally noted that data portability would also foster competition by facilitating switching between different service providers, and therefore promote development of new services, EU data protection commissioners, meeting as the Article 29 Data Protection Working Party, have released Guidelines on the right of data portability[30]. These Guidelines controversially proposed a broad interpretation of data 'provided by' a data subject and as to when it is 'technically feasible' to directly provide the data electronically to another service provider at the request of the data subject. Data 'provided by' the data subject includes data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.) – that is, 'volunteered data' - and data observed through use of a service or device where the data subject has consented to that data being collected and observed – 'observed data'. Examples provided in these Guidelines of observed data include a person's transaction history, internet search history, traffic data and location data and other raw and collated data such as the heartbeat tracked by a wearable device.

Thus, the EU data protection commissioners interpret the term 'provided by' to include personal data that relates to the data subject activity or results from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour, such as personal data created by the data controller as part of the data processing (e.g. by a personalisation or recommendation process, by user categorisation or profiling). In particular, observed data does not include 'inferred data' or 'derived data' created by a service provider – as a result, the right of portability only applies to data that a data subject has consented to be collected, and not information derived and transformed from that data.

The revised EU Payment Services Directive[31] (**PSD2**) mandates banks to "open up" payment account access to third parties to enable real-time payments by end of 2017. PDS2 also permits the aggregation of a consumer's account information in one place by an aggregator. No specific approach, such as APIs, has been mandated. This has led to an active and continuing debate as to whether screen scaring should be prohibited and also as to whether particular API standards should be mandated.

PSD2 makes a distinction between two types of services: payment initiation services and account information services. A 'payment initiation service' is a service to initiate a payment order with respect to a payment account held at another payment service provider. An 'account information service' is an online service to provide consolidated information on one or more payment accounts with either another payment service provider or with more than one payment service provider.

So-called 'account servicing payment service providers' (such as banks) will be (at least in principle) obliged to provide access to providers of payment initiation or account information services, provided that the relevant payment accounts are accessible online and the third party service provider is duly licensed. Banks may not require contracts with the third party service provider in order to have account-access. As under the current PSD, PSD2 qualifies a 'payment account' as an account held in the name of one or more payment service users which is used for the execution of payment transactions. In guidance in the context of PSD1, the European Commission explains[32] that the definition of payment account covers all accounts where the holder can place and withdraw funds without any additional intervention or agreement of his payment service provider such as current accounts. For example, when one account combines mortgage, saving and payment facilities in order to reduce the overall mortgage balance, this is considered to be a 'payment account'. Also, a saving account where the holder can place funds whenever he wants, without having to sign a new contract for each new placement, and is also able to withdraw funds whenever he likes without any restrictions (e.g., penalties associated with early withdrawal of a term deposit) should be considered as payment account for the purposes of the PSD.

[30] WP242 rev 0.1 as revised on 5 April 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44099

[31] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[32] European Commission, Q&A on the PSD http://ec.europa.eu/finance/payments/docs/framework/transposition/faq_en.pdf.

The UK Financial Conduct Authority (FCA) has taken a similarly expansive view. Under FCA guidance, 'payment accounts' can include:

- current accounts,
- e-money accounts,
- flexible savings accounts,
- credit card accounts, and
- current account mortgages.[33]

The fact that the definition of 'payment account' has not been further clarified under PSD2, will no doubt lead to 'interesting' legal debates between banks and third party service providers.

In the United States of America, the 2010 *Dodd-Frank Wall Street Reform and Consumer Protection Act* provided for consumer rights to access their financial records and account-related information and specified that this information "shall be made available in an electronic form usable by consumers". That statute also gave rulemaking authority over this area to the Consumer Financial Protection Bureau (**CFPB**).

In November 2016 the CFPB launched an inquiry "into the challenges consumers face in accessing, using, and securely sharing their financial records".[34] As at August 2017 the CFPB was still proposing to writing new rules to facilitate this data access, but it remained unclear whether such initiatives would be supported by the Trump Administration or, indeed, whether the CFPB would continue to be funded. In November 2016, the Federal Communications Commission had released stringent privacy rules and new disclosure requirements as to uses by carriers and broadband services providers of telecommunications customer data. These were eliminated by Congressional joint resolution signed into law by President Trump in April 2017.

11 New regulatory constructs as to consumer rights to data

The United Kingdom has set the global benchmark for regulatory intervention to assist consumers with access to basic transaction data to assist customer price comparisons and facilitate easier switching between service providers. However, UK regulatory intervention to date has been relevantly limited to core sectors, being energy supply, the mobile phone sector and larger banks.

The then United Kingdom Government commenced its midata initiative in early 2011 as a voluntary scheme applicable to customer transaction data in these core sectors.[35] The UK Government stated that two main benefits would arise from the new right. First, midata would help consumers make better choices: with access to their transaction data in an easy to use format, consumers would be able to make better informed decisions, often with the help of a third party. This in turn would reward firms offering the best value products in particular markets, allowing them to win more customers and profits and resources. Secondly, midata would be a platform for innovation: midata would lead to the creation of new businesses which will help people to interact with their consumption data in many innovative ways. Accordingly, midata was seen as delivering both demand-side and supply-side benefits: better information for consumers to make better choices, and stimulation of innovative service offerings on the supply side to provide consumers with an expanded range of services and service types.

[33] FCA, FCA Handbook, PERG 15.3 Payment Services https://www.handbook.fca.org.uk/handbook/PERG/15/3.html?date=2016-02-03.

[34] https://www.consumerfinance.gov/about-us/newsroom/cfpb-launches-inquiry-challenges-consumers-face-using-and-securely-sharing-access-their-digital-financial-records/. Se further Penny Crossman, 'Data-sharing debate grows contentious as fintechs vent grievances', *American Banker* 15 August 2017

[35] Department for Business, Innovation & Skills and The Rt Hon Edward Davey, The midata vision of consumer empowerment, November 2011, https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment

In April 2013 the *Enterprise and Regulatory Reform Act* gave the Secretary of State the ability to issue regulations imposing a duty on suppliers to provide customer transaction data to their customers in those 'core sectors' but also with the ability to extend this requirement to any supplier of goods and services.

In August 2016 the Competition and Markets Authority (**CMA**) required the largest U.K. banks to develop by 2018 a new open API banking standard that will enable customers and SMEs to share information with third parties including price comparison websites and the third party payment service providers created by PSD 2 (account information service providers and payment initiation service providers).[36] As currently scoped, it appears that this requirement would not apply to the full range of 'payment accounts' to which PSD 2 would apply and would only apply in respect of larger UK banks: the so-called 'High Street' banks RBS, Lloyds, Barclays, HSBC, Santander, Nationwide, Danske, Bank of Ireland and Allied Irish Bank. Certain less least sensitive information (for example, about prices, charges, terms and conditions and customer eligibility criteria) was required to be released by 31 March 2017. The CMA's final order[37] stated how recommendations it made following its retail banking market investigation should be implemented. The CMA's order requires the standards to be developed using open application program interfaces (APIs) and conform to standards on data formatting and security, including for authorisation and authentication.

To summarise the current position in certain key jurisdictions:

- **Europe** (European Commission) (including the UK pre-Brexit[38]): PSD2 directive mandates banks to "open up" payment account access to third parties to enable real-time payments. PSD2 also permits the aggregation of a consumer's account information in one place by an aggregator. No specific approach e.g. APIs has been mandated.[39] Implementation required by 18 January 2018.

- **United Kingdom** (CMA and Open Banking Working Group):

  Phase 1: "Minimum Viable Product" (value, data and direction of transaction only). End 2016

  Phase 2: Read-only personal customer transaction data ('Midata' data sets, i.e. bank statement with 12 months history). End Q1 2017.

  Phase 3: Full scope (Personal and Business Current Account Transaction Data and Lending Products Data, but excludes Insurance, Merchant Acquiring, Hedging and Foreign exchange.). Implementation required by 18 January 2018.

- **U.S.A.**: Awaiting fate of CFPB proposals (as above).

- **Singapore (Monetary Authority of Singapore)**: There is no government mandate for Open Banking APIs. The MAS has urged banks to adopt APIs and is implementing Open APIs to provide access to its own data. The Association of Banks in Singapore has published a Financial World: Finance-As-A-Service API PlayBook which was developed in consultation with MAS. The PlayBook "provides guidance to financial institutions, FinTech players and other interested entities in developing and adopting open Application Programming Interface (API) based system architecture".[40]

The state of play might be summarised as follows:

---

[36] https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-report

[37] *The Retail Banking Market Investigation Order 2017*, https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf

[38] HM Treasury, Implementation of the revised EU Payment Services Directive (PSDII) https://www.gov.uk/government/consultations/implementation-of-the-revised-eu-payment-services-directive-psdii.

[39] Both banks and new entrants in financial services technology are actively engaged in an industry-wide effort to develop common processes and standards. The forum for this cooperation is the Working Group on Payment Initiation Services of the Euro Retail Payments Board, created by the European Central Bank.

[40] ABS-MAS Financial World | Finance-as-a-Service: API PlayBook, https://abs.org.sg/industry-guidelines/fintech

- There is still no clear international consensus as to what 'open banking' means. In particular, regulators appear to differ about how to set the balance between regulatory initiatives to address information asymmetries affecting customer evaluation of alternatives and switching decisions –demand side initiatives – and regulatory initiatives to facilitate data flows to fintechs –supply side initiatives.

- There are legitimate information security concerns, often expressed in a debate as to restrictions on fintech screen scraping or facilitating screen scraping for fintechs, as compared to open APIs, as compared to contractually 'controlled release' APIs.

- There is significant debate as to the appropriate data specification and in particular the appropriate minimum data sets that should be 'opened'. This debate is often framed around consumer rights to their data, and sometimes expressed as a privacy debate, when the really hard question is often masked or ignored. That hard question is the question of whether, and if so when, a regulator may mandate access to valuable commercial-in-confidence information a bank holds about its customers in order to facilitate the regulator's vision of what 'open banking' should be. Partly the issue is that applicable law relating to ownership rights in confidential information in data bases is still developing in most jurisdictions. Partly the issue is that regulators are rightly concerned about getting the settings wrong and allowing new entrants to cherry pick and free-ride upon incumbent's valuable data.

12 Open banking in Australia

As most readers of this paper will be aware, on 9 May 2017 the Australian Treasurer The Hon Scott Morrison made a number of key announcements as to 'Building an accountable and competitive banking system'[41]:

- The Government will introduce an open banking regime that will increase access to banking product and consumer data by consumers and third parties, if the consumer consents.

- The Treasury will commission an independent review (budget $1.2m) to recommend the best approach to implement the open banking regime in Australia, to report by the end of 2017.

- The PC to commence a review on 1 July 2017 of the state of competition in the financial system, to report by 1 July 2018.

- The Government is also supportive of a phased approach to licensing banks. The Government welcomes APRA's review of prudential licensing arrangements and APRA's consideration of such approaches.

- The Government will act reduce regulatory barriers to entry for new and innovative entrants to the banking system. For those entrants the Government will relax the legislative 15 per cent ownership cap, whether through the existing ministerial discretion or legislative change. The prohibition on the term 'bank' by ADIs with less than $50 million in capital will also be lifted by legislation to allow them and other ADIs to benefit from the reputational advantages of the term.

- The ACCC will receive $13.2 million over four years to establish a dedicated unit to undertake regular in-depth inquiries into specific financial system competition issues.

- The Government will legislate a mandatory comprehensive credit reporting regime if credit providers are not reporting at least 40 per cent of their data by the end of 2017.

Notably, this announcement pre-empted the outcomes of the Australian Government's own taskforce that is in the course of reviewing the Productivity Commission's *Data Availability and Use Final Inquiry Report* of March 2017[42] to advise the Government as to whether to accept recommendations of that

[41] http://sjm.ministers.treasury.gov.au/media-release/044-2017/

[42] http://www.pc.gov.au/inquiries/completed/data-access/report

Report.[43] As a result we now have a two-speed process for review of access to consumer data in Australia: a fast-track for open banking (to report to the Treasurer by the end of 2017) and a slower track for all other sectors of the economy, notably including the now politically sensitive retail energy sector.

The Treasurer's *Terms of Reference for the Open Banking Review* are as follows[44]:

1.The review will make recommendations to the Treasurer on:

1.1. The most appropriate model for the operation of open banking in the Australian context clearly setting out the advantages and disadvantages of different data-sharing models.

1.2. A regulatory framework under which an open banking regime would operate and the necessary instruments (such as legislation) required to support and enforce a regime.

1.3. An implementation framework (including roadmap and timeframe) and the ongoing role for the Government in implementing an open banking regime.

2.The recommendations will include examination of:

2.1. The scope of the banking data sets to be shared (and any existing or potential sector standards), the parties which will be required to share the data sets, and the parties to whom the data sets will be provided.

2.2. Existing and potential technical data transfer mechanisms for sharing relevant data (and existing or potential sector standards) including customer consent mechanisms.

2.3. The key issues and risks such as customer usability and trust, security of data, liability, privacy safeguard requirements arising from the adoption of potential data transfer mechanisms and the enforcement of customer rights in relation to data sharing.

2.4. The costs of implementation of an open banking regime and the means by which costs may be imposed on industry including consideration of industry-funded models.

3.The review will have regard to:

3.1. The Productivity Commission's final report on Data Availability and Use and any government response to that report.

3.2. Best practice developments internationally and in other industry sectors.

3.3. Competition, fairness, innovation, efficiency, regulatory compliance costs and consumer protection in the financial system.

In August 2017 the Open Banking Review released an *Issues Paper*[45] proposing to define open banking for the Review as follows:

> Open Banking refers primarily to giving customers greater access to and control over their own banking data. Open Banking can be distinguished from 'open data', which refers to data that is available, typically on the internet, that anyone can access, use or share without the need to obtain consent. Rather, Open Banking enables the customer to direct that they, or third parties chosen by them, be provided with pre-determined parts of their banking data in a secure

[43] Data Availability and Use Taskforce. See https://www.pmc.gov.au/public-data/data-availability-and-use-taskforce

[44] https://www.treasury.gov.au/ConsultationsandReviews/Reviews/2017/Review-into-Open-Banking-in-Australia/Terms-of-reference

[45] www.treasury.gov.au/.../Consultations%20and%20Reviews/Reviews%20and%20Inqui...

environment and in a prescribed way, so that it can be used to offer them new or better services, such as:

• more competitive banking products that better suit their needs, or banking products that would otherwise not have been available to them, or

• better personal financial management, accounting, tax and budgeting tools.

The term is also used to refer to enabling open access to banks' data on their products and services.

More relevantly to this paper, the Issues Paper states:

> The right to direct that data be transferred could be made available to a broad range of customers, or applied in a more restricted way. The broader the range of customers who can initiate instructions to access data, the greater the benefit, and the greater the regulatory burden. The right could be restricted to individuals, or include some businesses. If the right to seek access to data includes small businesses, for example, an appropriate definition would need to be adopted and that status would need to be verifiable by the respective data provider.
>
> Finally, with whom data can be shared and how data is used will be important. Enabling third parties (such as FinTech companies) to develop new banking products and services for banking customers that deliver enhanced outcomes - such as lower fees or lower loan interest rates - will be critical to realising the benefits of Open Banking. The Review may therefore consider mechanisms by which third parties can be identified for suitability to participate in the Open Banking regime.
>
> The terms of reference ask the Review to examine the mechanisms for sharing relevant data, including existing or potential sector standards. As part of that examination, the Review will consider whether it is appropriate to set out specific data transfer standards and, if so, the best model for defining those standards.
>
> The Review will also consider specifications and rules (including legal frameworks) to govern the data transfer process in order to provide appropriate protections for customers, whilst being flexible enough to accommodate future technological innovation. The Review may also take into account whether such specifications and rules would allow for broad participation or would create barriers to entry that could risk excluding certain players from participation.
>
> Determining how a data transfer request is to be initiated by the customer and how that data is to be shared will be an important step in establishing a successful Open Banking regime in Australia. As customers should be able to require their bank to share their data directly or with a third party chosen by them, the Review will consider how to ensure that the customer should become properly aware of the terms of access and use of their shared data.

The Issues Paper calls for submissions to be lodged by 22 September 2017.

13 Productivity Commission Data Availability and Use Final Inquiry Report

As has been widely reported, the Australian Productivity Commission *Data Availability and Use Final Inquiry Report*[46] of 9 May 2017 included radical proposals for access to consumer data. No other regulatory jurisdiction has proposed economy wide mandated access of consumers to 'consumer data' as broadly (proposed to be) defined. We have already noted that the Australian Government has established a Taskforce[47] to review the Final Inquiry Report and advise Government as to whether to accept recommendations in that Report. It is not currently expected that the Taskforce will engage in further public consultations. The Government is expected to announce its views on the recommendations in the Final Inquiry Report sometime in Q4 2017.

[46] Available at http://www.pc.gov.au/inquiries/completed/data-access#report.

[47] Data Availability and Use Taskforce. See https://www.pmc.gov.au/public-data/data-availability-and-use-taskforce

There is very little discussion in the Productivity Commission's report as to operation of proprietary rights and quasi-property concepts such as rights to confidential information or trade secrets.

> Broadly speaking, the intent of the Comprehensive Right is to facilitate enhanced competition and innovation. Taking account of the substance, if not the literality, of these participant comments, it is our intention that the new Right would operate within the bounds of Australia's intellectual property right arrangements, as described in chapter 1.
>
> For clarity, however, we do not consider that data that has been cleansed of errors, made better through simple statistical means such as aggregated or averaged for each consumer but otherwise unaltered, or made machine-readable could singly or collectively be construed to be value added (as some might argue).

The Productivity Commission put forward a broad outcome-focused scope for determination (not a definition) of 'consumer data', being *the type of data held on a consumer or SME that a competing or complementary business would themselves need, and reasonably expect to obtain, in order to make a reasonable offer for a consumer's patronage*.

The Commission recommended that an industry data-specification process should be established "to review and reach agreement on the exact definition of consumer data for that industry (based on an understanding of the relevance of specific types of data for provision of a consumer product or service in that industry). This would allow the scope of the Right to move with the march of technology/data, as is highly desirable for any regulation. And, in the absence of industry agreement, the broadest level definition of consumer data would apply as the default, for that industry."

The Commission saw "the flexibility inherent in an outcome-based definition and data-specification process" as appropriate to allow for industry or sectoral variations to the definition of data and to avoid "mandating provision of data that is of no use to consumers, for transfer of their custom, in a particular industry".

Where requested by industry or the ACCC, an officer from an agency of the Treasury portfolio could be a member of the industry data-specification group. "This might allow, for example, the Australian Securities and Investment Commission (ASIC) or the Reserve Bank of Australia (RBA) to participate in the banking sector data-specification process."

> In addition to defining the scope of consumer data, data-specification agreements should also articulate: transfer mechanisms, including security protocols, to ensure that data handling is practical and robust to technology updates; and the requirements necessary to authenticate a consumer request prior to any transfer. This means that industries would be able to tailor (with agreement) data security requirements for their particular sector — such an approach recognises that data sharable in each sector is likely to have different risks, and therefore different approaches to managing these risks. In practice, this means that parties would have responsibility only for the data they hold, not for data they have transferred to a third party at the consumer's direction — that responsibility should lie with the third party.
>
> The industry-agreed definition of consumer data, including agreed transfer mechanisms and security protocols, should be registered with the ACCC, who would assess whether the definition would be sufficient to achieve the intended outcomes (in terms of what consumers should be able to obtain from the new Right).

In the absence of industry agreement on the definition of consumer data, "all data included in the broad level default definition above would be deemed relevant to a consumer's request for their data from an entity in that industry. The ACCC would determine, through the presence or absence of registered industry data-specification, what level of access a consumer was entitled to should a dispute arise. And in the absence of an industry agreement, security arrangements to be applied for that industry would be the default security protocols established by Government. Given that the right would apply across the economy, sectors would need to be prioritised in registering their definition of consumer data with the ACCC, who should be allowed to offer interim approval where a data-specification is ready but there are higher priority sectors drawing the regulator's attention."

Where the consumer right operated in relation to consumer data within the data specification for a particular industry, the elements of that right were proposed to be:

- to access a copy of this data, regardless of whether:

  – provided directly by the consumer,

  – collected in the course of other actions (and including administrative datasets) and identifiable to that consumer (whether aggregated or not), or

  – held by the data holder even though created by others - for example through screen-scraping or tracking, purchase of data about a consumer, or re-identification, and

- to request edits or corrections for reasons of accuracy,

- to direct holders of such data to copy the data in machine-readable form, either to the consumer directly or to a nominated third party (the 'transfer right'),

- to be informed about the trade of any element of this data to third parties, and

- to be advised of disclosures of data to third parties.

14 Conclusion

We should expect to see the debate as to consumer access to data and data portability to become better framed in terms of finding the balance between promoting consumer trust and promoting competition.

Consumer trust is a key attribute of the social contract between individuals (consumers and citizens) and businesses and governments that enables use and limited sharing of information about individuals. Consumer trust is also integral to adoption of many efficiency enabling technologies and services and therefore to achievement of the benefits to society that are expected to flow from uptake of these technologies and services.

Rights of access to data and of data portability nurture consumer trust, by lifting confidence over time that consumers, along with governments and businesses, can choose how and when to use their own data. But it will often be difficult to determine the appropriate point beyond which data ceases to be about customer transactions and should then be protected from disclosure as commercial-in-confidence business information. As business investment in data analytics increases, it becomes even more important to get this point right.

Incorrect regulatory settings will undermine incentives for services providers to innovate by value-adding in service feature and functionality and improving personalisation of services by data analytics and data transformations.

Incorrect settings may facilitate free riding by less innovative service providers upon innovations by first movers, and unfairly appropriate or undermine trade secrets and other intellectual property of first movers.

Also, the significant costs in implementation of APIs for access to data are a cost burden on businesses that must be balanced against consumer benefit: there may be relatively few industry sectors and service providers where cost-benefit analysis supports mandating API enabled access to data and data portability.

The battles now being fought over consumer data will continue to be fought over the next few years. It is clear that the outcome will be increased consumer access to data and technological support for electronic data portability. But the ways in which that access will be provided, and the extent to which

access will be mandated through regulatory action either in particular industry sectors or across economies, remain hotly in contention.

Peter G Leonard

Principal, Data Synergies
Consultant, Gilbert + Tobin

M +61 411 089 003
E pleonard@datasynergies.com.au
LI https://www.linkedin.com/in/peleonard/

30 August 2017

Attachments

Screen Scraping Terms – Example #1 - Realestate.com.au
www.realestate.com.au
https://about.realestate.com.au/terms-use/

Restrictions on use of websites

In accessing or using our platform you agree that you will not:

(a) use any automated device, software, process or means to access, retrieve, scrape, or index our platform or any content on our website;

(b) use any device, software, process or means to interfere or attempt to interfere with the proper working on our website;

(c) undertake any action that will impose a burden or make excessive traffic demands on our infrastructure that we deem, in our sole discretion to be unreasonable or disproportionate site usage;

(d) use or index any content or data on our platform for purposes of:

(i) constructing or populating a searchable database of properties,

(ii) building a database of property information; or

(iii) competing with us in any manner that we have not specifically authorised;

(e) transmit spam, chain letters, contests, junk email, surveys, or other mass messaging, whether commercial in nature or not;

(f) use our platform or any content from our platform in any manner which is, in our sole discretion, not reasonable and / or not for the purpose which it is made available;

(g) violate the rights of any person, including copyright, trade secret, privacy right, or any other intellectual property or proprietary right;

(h) pose as any person or entity or attempt to solicit money, passwords or personal information from any person;

(i) act in violation of any Term of Use or other condition posed by us or any applicable law;

(j) reproduce, republish, retransmit, modify, adapt, distribute, translate, create derivative works or adaptations of, publicly display, sell, trade, or in any way exploit our platform or any content on our website, except as expressly authorised by us; or

(k) transmit or attempt to transmit any computer viruses, worms, defects, Trojan horses or other items of a destructive nature.

We reserve the right to exercise whatever means we deem necessary to prevent unauthorised access to or use of our website, including, but not limited to, instituting technological barriers, or reporting your conduct to any person or entity.

Screen Scraping Terms – Example #2 - SEEK Limited
https://www.seek.com.au/terms/

Information for personal, non-commercial use only

You agree that information contained on this Site is for personal use only and may not be sold, redistributed or used for any commercial purpose (this includes but is not limited to the use of

Advertiser contact details for unsolicited commercial correspondence and the information available via our insights and resources subdomain https://insightsresources.seek.com.au/). You may download material from this Site for your personal, non-commercial use only, provided you keep intact all copyright and other proprietary notices.

You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any material from this Site including code and software. You must not use this Site for any purpose that is unlawful or prohibited by these terms of use.

You may not use data mining, robots, screen scraping, or similar automated data gathering, extraction or publication tools on this Site (including without limitation for the purposes of establishing, maintaining, advancing or reproducing information contained on our Site on your own website or in any other publication), except with Our prior written consent.

Video of EBF on screen scraping

http://www.ebf.eu/what-is-screen-scraping/

Video of European Banking Federation on banking APIs

http://www.ebf.eu/what-do-apis-mean-for-banking/

EBF asks Commission to support ban on screen scraping

http://www.ebf.eu/ebf-asks-commission-to-support-ban-on-screen-scraping/

Privacy of client data, cybersecurity and innovation at risk if EBA standards are dismissed and screen scraping continues

BRUSSELS, 16 May 2017 – The European Banking Federation has asked the European Commission not to dismiss a key recommendation by the European Banking Authority (EBA) on future electronic payments in the European Union. The EBF fears that the privacy of client data, cybersecurity and innovation are put at risk if the Commission does not fully endorse the EBA standards.

PSD2 introduces a general security upgrade for third-party access to a client's data, bringing an end to practices known as 'screen-scraping'. Such services, seen as a first-generation direct access technology, let third parties access bank accounts on a client's behalf by impersonating while using their access credentials. PSD2 calls for the creation of a technology-neutral level-playing field for banks and fintechs, new and old.

The proposal requires banks to opt for either creating a 'dedicated interface' that lets third parties access bank accounts on behalf of clients, or to upgrade their client interface. These solutions would replace the old practice of screen-scraping. They ensure the continuation of direct access services in the EU in a secure way by empowering clients to decide for themselves which data can be accessed by third parties. The EBF sees the EBA standards as a common solution that ensures security and as a significant catalyst for innovation into the future in the European payments market, fully compliant with the EU's General Data Protection Regulation (GDPR).

The European Commission appears to be willing to go against the EBA advice and may let screen-scraping continue by requiring banks to accept screen-scraping as an additional mandatory direct access method, forcing banks to maintain at least two interfaces. Banks are deeply concerned over this development and fear that such a choice would harm the development of electronic payment services. It would come at the expense of innovation in payment services and would make it more difficult to protect the privacy of account holders.

Says Wim Mijs, Chief Executive Officer of the EBF:

"The development of PSD2 can be compared to designing a new plane. You develop highly secure, innovative and sophisticated systems to make it fly. But what happens now, in the final development

stages, is that the designers are required to put a heavy diesel generator on board. This plane then becomes too heavy to fly. If banks are forced to accept screen–scraping then PSD2 will never fly the way it was intended."

Both banks and new entrants in financial services technology are actively engaged in an industry-wide effort to develop common processes and standards. The forum for this cooperation is the Working Group on Payment Initiation Services of the Euro Retail Payments Board, created by the European Central Bank.

About the EBF:

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks – large and small, wholesale and retail, local and international – employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

Banks support ecosystem of interoperable APIs in EU

http://www.ebf.eu/ebf-statement-on-eu-commission-position-on-eba-rts-for-psd2/

BF underlines importance of privacy and security under PSD2

BRUSSELS, 2 June 2017 – In the context of the second EU Payment Services Directive (PSD2) the European Banking Federation would like to underline that banks in the European Union fully support the creation of an efficient and effective EU ecosystem of interoperable interfaces for secure and reliable communication via the banks' infrastructure between third-party payment service providers, known as TPPs, and clients.

Customers expect banks to protect their personal data. Data protection is at the core of trust in financial institutions. That is why the EBF, taking note of the European Commission's response to the European Banking Authority (EBA) on its regulatory and technical standards for strong customer authentication under PSD2, would like to reiterate its concerns over the consequences of the amendment proposed by the European Commission.

Even though TPPs would have to identify themselves towards banks, they would still have access, at minima, to all the balances of all the accounts held by clients when clients pay on the internet through the existing practice known as 'screen scraping'. The privacy of client data, cybersecurity and innovation are all at risk if 'screen-scraping' is allowed to continue once PSD2 enters into force next year. Clients must be able to choose which account data they want to share with payment service providers and which not. When a TPP accesses consumer accounts via 'screen scraping' services, even when identifying themselves to a bank, consumers are still not able to contain this TPP access to their account information, thus endangering the privacy of their data.

Banks instead favour an EU ecosystem for third-party access to consumer account data that is secure, reliable and interoperable, either through introducing Application Programming Interfaces, or APIs, or by upgrading existing bank interfaces. Only thus can TPP access be contained to only the data for which the consumer has given explicit consent. Such new and innovative financial technology would ensure compliance with the EU's new privacy requirements under the General Data Protection Regulation (GDPR) that enters into force in May 2018. Banks in several EU Member States have already developed sector-wide APIs for third-party access to client accounts.