NUS Centre for Banking & Finance Law Working Paper 20/03

NUS Law Working Paper 2020/024

Open Banking: The Changing Nature Of Regulating Banking Data - A Case Study Of Australia And Singapore

Emma Leong

Centre for Banking & Finance Law, Faculty of Law, NUS

First published in the Banking & Finance Law Review

July 2020, Issue 35.3, pp 443 - 469

[uploaded August 2020]

Published in the Banking & Finance Law Review
July 2020, Issue 35.3, pp 443 - 469

OPEN BANKING: THE CHANGING NATURE OF REGULATING BANKING DATA A CASE STUDY OF AUSTRALIA AND SINGAPORE

Emma Leong*

Abstract

Historically, the banking relationship is envisaged as a closed one between bank and customer. However, the advent of open banking has challenged that closed model. Open banking involves the sharing of customer data with third parties as directed and initiated by customers. This sharing assumes that customers "own" their banking data and should therefore reap the benefits of such ownership. This article considers two very different frameworks and analyses how conducive they are to an open banking paradigm. The first is a duty–based framework comprising banking secrecy and data protection provisions; the second is a tailored rights–based framework that accords customers greater control over their banking data with open banking specifically in mind. The article concludes that, given the new ways in which banking data is used in an open banking paradigm, a rights–based framework that bolsters customer control over data is more conducive to open banking.

1. INTRODUCTION

Open banking is an emerging financial services model that focuses on the portability and open availability of customer data held by financial institutions.[1] An open banking framework comprises three key features: customers having greater access to and control over their banking data; financial institutions being required to share customer data with customers; and, with the consent of customers, financial institutions sharing customer data with accredited third party providers ("**TPPs**"), which may include competing providers of financial services.[2] This sharing of customer information is touted as giving customers control over their data, leading to greater choice in their banking service providers and more convenience in managing their money.[3] Open banking use–cases include account aggregation services that allow bank customers to view their accounts from different banks through a single interface, and product comparison services that enable customers to identify suitable financial products, both of which facilitate the management of personal finance.[4] Open banking is also marketed as a tool to tackle anti–competitive behaviour in the financial services industry. This discussion proceeds on the assumption that open banking is a positive development for customers.[5]

Globally, open banking has captured the attention of both traditional financial institutions and financial technology companies, changing the way in which banking data can be utilized. Results of a 2018 survey indicate that 77% of banks in Europe and 61% of banks across Asia Pacific are planning to invest

* Research Assistant, Centre for Banking and Finance Law, Faculty of Law, National University of Singapore. The author would like to thank Professor Sandra Booysen for her tireless review of this article. My thanks also to Professor Dora Neo, Jodi Gardner, Jin Sheng, Petrina Tan, Elson Ong, participants of the working paper presentation held on 29 August 2019 and the anonymous reviewers for their invaluable comments.

[1] Ana Badour & Domenic Presta, "Open Banking: Canadian and International Developments" (2018) 34:1 Banking and Finance Law Review 41.

[2] Philip Hamilton, "'You're more likely to divorce than switch banks': will Open Banking encourage more switching?" *Parliament of Australia* (17 July 2019), online: <https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2019/July/Open_Banking>.

[3] Australia, Commonwealth, The Treasury, *Review into Open Banking: giving customers choice, convenience and confidence* (Canberra: The Treasury, 2017) ("**Farrell Report**") at v.

[4] UK, The Open Data Institute and Fingleton Associates, *Open Banking, Preparing for lift off: Purpose, Progress & Potential* (London: The Open Data Institute and Fingleton Associates, July 2019) at 30.

[5] The proposition might not be universally true, see comments by Mick McAteer of the UK's Financial Inclusion Centre in Kevin Peachey, "Why banks will share your financial secrets" *British Broadcasting Corporation* (11 January 2018), online: <https://www.bbc.com/news/business-42253051>.

up to USD $20 million each to undertake open banking initiatives for commercial customers.[6] Open banking involves sharing data with TPPs through application programming interfaces ("**APIs**").[7] APIs are software protocols that determine how one application (such as a mobile phone, or web application) interacts with another, usually to facilitate an information exchange.[8] For any given software or application, an API specifies a mechanism for connecting to the software or application, the data and functionality made available to the software, as well as the rules and standards that need to be followed by other applications to interact with the application's data and functionality.[9] The sharing of data envisaged by open banking is juxtaposed against a fundamental tenet of banking law: a bank's duty of secrecy. Historically, the banking relationship is a private relationship between banker and customer. The novelty of open banking lies in its challenge to the historical model by promoting the sharing of the customer's transactional banking data with trusted third parties.[10] The development of open banking proceeds on the basis that customers own their banking data and should reap the benefits from such ownership by having it shared in ways that are beneficial to the customer. Given that open banking involves a shift away from the historically closed relationship between a bank and its customer, the question that follows is what features should a legal framework governing bank customer data exhibit, in order for open banking to flourish?

Different regulatory approaches have been taken towards open banking that can broadly be classified as mandatory, supportive and neutral.[11] In a mandatory jurisdiction, regulators have passed legislation to compel the adoption of open banking practices, while in supportive jurisdictions clear shifts have been made towards facilitating open banking without mandating it.[12] In neutral jurisdictions, there is an absence of regulatory statements on open banking but some industry–led adoption and experimentation.[13] In mandatory jurisdictions such as in Australia, third party providers are regulated as data recipients and specific rules have been set on how customer banking data is to be governed in an open banking paradigm. The focus here on the bank–customer relationship is warranted as the bank is the primary repository of customer information, but in a mandatory jurisdiction the legal framework has been expanded to include TPPs' rights and duties in accessing customer banking information. Consequently, there is greater clarity pertaining to the customer's rights over his/her banking data in relation to TPPs. In contrast, in supportive and neutral jurisdictions a customer's rights over his/her banking data is governed by pre–existing banking law and regulation and/or by general data protection legislation. In Singapore, a supportive jurisdiction, pre–existing banking secrecy and personal data protection regulation remain the relevant legislation underpinning open banking development. Such legislation was primarily drafted against the backdrop of a closed relationship between bank and customer and does not envisage the sharing of information with TPPs in an open banking paradigm. Hence, TPPs access a bank customer's information subject to the bank's existing legal obligations towards its customers' data. In developing open banking functionalities, the bank releases customer information to TPPs insofar it is compliant with banking secrecy and personal data protection

[6] Alan McIntyre, Hakan Eroglu & Andrew McFarlaneet al., *Accenture Open Banking for Businesses Survey 2018 - It's Now Open Banking Do You Know What Your Commercial Clients Want From It?* (2018) at 6-7, online: <https://www.accenture.com/_acnmedia/pdf-90/accenture-open-banking-businesses-survey.pdf>.
[7] Switzerland, Financial Stability Board, *FinTech and market structure in financial services: Market developments and potential financial stability implications* (Switzerland: Financial Stability Board, 2019) at 4.
[8] Singapore, The Association of Banks in Singapore & Monetary Authority of Singapore, *ABS-MAS Financial World: Finance-as-a-Service API Playbook* (Singapore: The Association of Banks in Singapore & Monetary Authority of Singapore, 2013) at 5.
[9] *Ibid.*
[10] James Black & Krista Koskivirta, "Open Banking - What is it and what is it good for?" (2018) Annual Banking Law Update 39.
[11] Microsoft, Linklaters & Accenture, "Open banking: A shared opportunity" *Microsoft* (2019), online: <https://www.microsoft.com/cms/api/am/binary/RE489V8> at 20.
[12] *Ibid.*
[13] *Ibid.*

regulation. The bank–customer relationship remains the primary legal relationship from which TPP access to customer information occurs in the supportive jurisdiction's open banking paradigm.

This article explores the implementation of the mandatory and supportive approaches in practice, utilising Australia's and Singapore's experience as case studies. Both jurisdictions have actively embraced the philosophy of open banking and are working out its practical implementation by using a mandatory and supportive approach respectively. The consequences of adopting each approach is considered and the relevant changes, or lack thereof, made to the legal framework governing a customer's banking data are examined. In supportive jurisdictions where open banking is encouraged but not compulsory, it is unlikely for both the bank and TPPs to be expressly regulated. Hence this article examines the extent to which the existing rights and duties of a bank regarding its customers' banking data, being the applicable legislative framework undergirding open banking in supportive jurisdictions, can support the growth of open banking. This examination may be illuminative for supportive or neutral jurisdictions considering which regulatory approach to adopt when implementing open banking[14] or for jurisdictions looking to refine their current approach. This article focusses solely on the applicable legislative frameworks in Singapore and Australia and does not evaluate the policy motivations for open banking,[15] nor does it seek to make a normative evaluation of whether open banking is a desirable development.

2. OPEN BANKING IN SINGAPORE AND AUSTRALIA

(a) Singapore

Singapore has adopted an "organic approach" towards open banking.[16] While it wants banks to share data with financial technology and other non–bank firms, its financial regulator, the Monetary Authority of Singapore ("**MAS**"), believes that the transition to open banking can be more successful without enacting legislation.[17] Hence, the *Banking Act*[18] and the *Personal Data Protection Act*[19] (the "***PDPA***") remain the primary statutes regulating banking data in Singapore. However, MAS has collaborated with the Association of Banks in Singapore to release non–binding guidance on developing and adopting open API–based system architecture which seeks to set data and information standards.[20] Singapore has been ranked by global financial software provider, Finastra, as top in the Asia–Pacific region for open banking readiness.[21] The survey takes into account Singapore's higher adoption of APIs, partnerships between banks and third parties, advanced data–based transformation, and innovation as primary factors.[22] Banks in Singapore have been active in API development. OCBC Bank was the first in

[14] Governments are grappling with an appropriate regulatory response to the implementation of open banking. For example, while Canada has completed the first stage of its review of open banking in May 2019, calls have been made for the federal government to move forward with more decisive action on a suitable open banking framework. See Christopher C. Nicholls, "Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation" (2019) 35:1 Banking and Finance Law Review 121; Ana Badour & Domenic Presta, "Open Banking: Canadian and International Developments" (2018) 34:1 Banking and Finance Law Review 41.

[15] For example, Australia's 2014 Financial System Inquiry recognized the role that increased data sharing could play in the development of alternative business models and products and services of the type that will improve consumer outcomes in financial services. See The Treasury, *supra* note 3 at 4-5.

[16] Chanyaporn Chanjaroen & Haslinda Amin, "Singapore Favors 'Organic' Policy in Move Toward Open Banking" *Bloomberg* (13 April 2018), online: <https://www.bloomberg.com/news/articles/2018-04-12/singapore-favors-organic-policy-in-move-toward-open-banking>.

[17] *Ibid.*

[18] *Banking Act*, (Cap. 19, 2008 Rev. Ed. Sing.) [*Banking Act*].

[19] *Personal Data Protection Act 2012* (No. 26 of 2012, Sing.) [*PDPA*].

[20] The Association of Banks in Singapore & Monetary Authority of Singapore, *supra* note 8 at 4.

[21] Leila Lai, "Singapore leads Asia-Pacific in Open Banking Readiness: Poll" *Business Times* (14 November 2018), online: <https://www.businesstimes.com.sg/banking-finance/singapore-leads-asia-pacific-in-open-banking-readiness-poll>.

[22] *Ibid.*

Southeast Asia to launch an open API platform in 2016,[23] while DBS launched an API developer platform in 2017 that is touted to be the largest by a bank anywhere in the world.[24] MAS has also partnered the International Finance Corporation and the ASEAN Bankers Association to launch the ASEAN Fintech Innovation Network[25] which has in turn launched the Industry Sandbox, an interoperable and scalable infrastructure acting as a method to standardize banking infrastructure and data.[26]

(b) Australia

The development of open banking in Australia has been primarily led by the Australian government. Since 2017, the Australian government has taken the position that an open banking regime that increases consumer and third party access to product and consumer data, will empower consumers to seek out banking products better suited to their needs, and create further opportunities for innovative business models in the banking sector.[27] Accordingly, in July 2017 the Australian government commissioned the Farrell Report to consider the optimal framework to implement open banking.[28] As a result of the review, the Farrell Report was produced, containing fifty recommendations on an ideal regulatory framework and how to implement it in the banking sector. The Farrell Report recommended that the implementation of open banking be primarily made through amendments to the *Competition and Consumer Act 2010*,[29] and for a national Consumer Data Right to be enacted which will allow customers open access to their banking transaction.[30] Public consultations on the *Treasury Laws Amendment (Consumer Data Right) Bill* were conducted from 2018, and the *Treasury Laws Amendment (Consumer Data Right) Act 2019* was enacted on 12 August 2019 to create Australia's Consumer Data Right ("**CDR**").[31] The *Treasury Laws Amendment (Consumer Data Right) Act 2019* is supplemented by the *Competition and Consumer (Consumer Data Right) Rules 2019*, drafted by the Australian Competition and Consumer Commission.[32] Moving forward, the four major banks in Australia[33] will be required to provide consumer, account and transaction data for credit and debit cards, deposit accounts, transaction accounts, and mortgage accounts to customers and accredited third parties by February 2020.[34]

---

[23] OCBC Bank, "OCBC Bank is the first bank in Southeast Asia to launch open API platform" *OCBC Group Newsroom* (17 May 2016), online: <https://www.ocbc.com/group/media/release/2016/first-bank-in-sea-to-launch-open-api-platform.html>.

[24] DBS Bank, "Reimagining banking, DBS launches world's largest banking API developer platform" *DBS Bank* (2 November 2017), online: <https://www.dbs.com/newsroom/Reimagining_banking_DBS_launches_worlds_largest_banking_API_developer_platform>.

[25] Monetary Authority of Singapore, "ASEAN Financial Innovation Network to support financial services innovation and inclusion" *Monetary Authority of Singapore* (16 November 2017), online: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/ASEAN-Financial-Innovation-Network-to-support-financial-services-innovation-and-inclusion.aspx>.

[26] Monetary Authority of Singapore, "World's First Cross-Border, Open-Architecture Platform to Improve Financial Inclusion" *Monetary Authority of Singapore* (18 September 2018), online: <https://www.mas.gov.sg/news/media-releases/2018/worlds-first-cross-border-open-architecture-platform-to-improve-financial-inclusion>.

[27] Australia, Commonwealth, The Treasurer, The Hon. Scott Morrison MP, *Building an Accountable and Competitive Banking System* (Canberra, Australia: The Treasury, 2017).

[28] Australia, Commonwealth, The Treasury, Consumer Data Right (Canberra, Australia: The Treasury, 2018).

[29] *Competition and Consumer Act 2010*, (No. 51 of 1974, Sing.).

[30] The Treasury, *supra* note 3 at vii. There are plans to extend this framework to energy, phone and internet transactions. Australia, Commonwealth, Assistant Minister for Cities and Digital Transformation, The Hon. Angus Taylor MP, *Australians to own their own banking, energy, phone and internet data* (Canberra, Australia: The Treasury, 2017).

[31] See full timeline at Australia, Commonwealth, The Treasury, *Consumer Data Right* (Canberra, Australia: The Treasury, 2019), online: <https://treasury.gov.au/consumer-data-right>.

[32] A lock down version of the Consumer Data Right Rules have been published on Australia, Commonwealth, Australian Competition & Consumer Protection Commission, *Competition and Consumer (Consumer Data Right) Rules 2019* (Canberra: Australian Competition & Consumer Protection Commission, 2019), online: <https://www.accc.gov.au/system/files/Proposed%20CDR%20rules%20-%20August%202019.pdf >.

[33] Namely Commonwealth Bank of Australia, Westpac Banking Corporation, Australia and New Zealand Banking Group, and National Australia Bank, collectively the "**Big Four Banks**".

[34] The Treasury, *supra* note 28.

3. REGULATING CUSTOMER BANKING DATA IN OPEN BANKING: EVALUATING EXISTING FRAMEWORKS

Given the challenge that open banking poses to the historical model of a banking relationship as a private relationship between banker and customer, it is pertinent to evaluate the extent to which existing legal frameworks are able to facilitate the sharing of customer information in an open banking situation. Generally, the scope of duties that a bank owes to its customers to keep his/her information confidential are primarily found in banking common law and/or legislation. The development of data protection laws in the 1970s have also resulted in banks being increasingly subject to overlapping but different ranges of obligations relating to the protection of customer information.[35] Broadly speaking, both banking secrecy and data protection laws seek to protect a bank customer's data by restricting the bank's use of such data.

In the common law world, the seminal English case on a bank's duty of secrecy, *Tournier v. National Provincial and Union Bank of England*[36] largely applies. The *Tournier* duty of secrecy is an implied contractual duty applicable to banks across common law countries such as Hong Kong and Canada.[37] Banks owe a duty to safeguard customer information, and disclosure is permitted only within four exceptions: where disclosure is required by law; where it is necessary for the fulfilment of a public duty; where it is in the interests of the bank; and where it is done with the customer's express or implied consent.[38] In Singapore, a bank's duty of secrecy was based on *Tournier* until it was captured in the *Banking Act*, s. 47. The provisions of the *PDPA* also govern the use and disclosure of bank customer information. As Singapore has not passed legislation specifically to facilitate open banking, the *Banking Act* and the *PDPA* remain the primary statutes governing banking data.

The common law *Tournier* duty of secrecy is also applicable in Australia. Australia has not legislated on banking secrecy. However, federal, state and territory laws on data protection may be relevant. For example, at a federal level the *Privacy Act 1988 (Cth)*[39] regulates the handling of personal information and is applicable to private sector entities with an annual turnover of at least AUD three million, including banks.[40] However, the pre–existing legal framework governing banking data was deemed inadequate to facilitate the development of open banking. For example, it was held that consent for the use of banking data in open banking should contain elements beyond the requirements of the *Tournier* exceptions and the *Privacy Act*.[41] Hence, the enactment of the CDR was subsequently proposed to support the growth of open banking.

The remainder of this section evaluates the extent to which existing, pre–open banking legal frameworks such as the common law *Tournier* duty, the approach taken in Singapore's *Banking Act*, and in Singapore's *PDPA* are able to facilitate open banking. In doing so, this section will evaluate the conceptual basis for such legal frameworks, the type of data governed and how information is shared in such frameworks.

(a) Conceptual Bases for the Duties of Secrecy and Data Protection

In *Tournier*, Bankes LJ explained that the basis for a bank's duty to ensure the confidentiality of the relationship between the banker and its customer is an incident of the law of agency.[42] The bank's duty

---

[35] Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (Oxford, UK: Oxford University Press, 2014) at 31.
[36] *Tournier v. National Provincial and Union Bank of England*, [1924] 1 K.B. 461, 130 L.T. 682 [*Tournier*].
[37] Dora Neo, "A Conceptual Overview of Bank Secrecy" in Sandra Booysen & Dora Neo, eds., *Can Banks Still Keep A Secret? - Bank Secrecy in Financial Centres Around the World* (Cambridge, UK: Cambridge University Press, 2017) 3 at 9.
[38] *Tournier, supra* note 37 at 473.
[39] *Privacy Act 1988* (No. 119, 1988, Sing.).
[40] *Ibid.,* ss. 6, 6C & 6D.
[41] The Treasury, *supra* note 3 at 60.
[42] Peter Ellinger, Eva Lomnicka & Christopher Hare, *Ellinger's Modern Banking Law,* 5th ed. (Oxford, UK: Oxford University Press, 2011) at 171-172.

of secrecy is important because "the credit of the customer depends very largely upon the strict observance of that confidence."[43] In Singapore, the *Tournier* duty preceded a legislative formulation of the duty of secrecy in the *Banking Act*. Commenting on the policy behind section 47, Professor Peter Ellinger has stated that it appears to protect a customer's privacy as long as it does not pervert the course of justice or the efficacy of banking operations.[44] Section 47(1) of the *Banking Act* prescribes that a bank shall not disclose customer information to any third party unless expressly permitted by the *Banking Act*. These exceptions are found in the Third Schedule of the Act. The Third Schedule permits the disclosure of information in a stipulated range of circumstances, such as where a customer has given written consent; in connection with a customer's insolvency; or where disclosure is required by law such as in compliance with the *Deposit Insurance and Policy Owners' Protection Schemes Act 2011*.[45] Section 47(6) of the *Banking Act* reinforces the strict duty of secrecy by imposing a maximum of a $125,000 fine or three year imprisonment on any individual, or a maximum of a $250,000 fine on any corporation that breaches the section 47(1) duty. Collectively, section 47 and the Third Schedule impose a strict minimum standard governing the bank's duty of secrecy. It is notable that a 2001 revision of the *Banking Act* resulted in a new section 47(8), reinforcing the minimum standard set for banking secrecy by the *Banking Act* and allowing a higher standard of secrecy to be imposed by entering into a private arrangement.

Similarly, the data protection regime in Singapore set out in the *PDPA* generally restricts the use and disclosure of personal data. While not industry–specific, the *PDPA* imposes obligations on "organisations"[46] which includes banks operating in Singapore. Under the *PDPA*, data protection is accorded only to individuals, defined as natural persons whether living or deceased.[47] The overarching objective of the *PDPA* is set out at section 13, which states that an organisation must not collect, use or disclose an individual's personal data unless it is legally required or there is express or deemed consent from the individual. Conceptually, the *PDPA* restricts the flow of personal data except where the statutory minimum conditions have been met. This approach is aligned with section 47 of the *Banking Act*, which prohibits the disclosure of customer information subject to the Third Schedule carve outs. The *PDPA* has been conceptualized by Professor Simon Chesterman as a "pragmatic attempt to regulate the flow of information, moderated by the touchstone of reasonableness."[48] For example, the *PDPA* imposes a duty on organisations to protect personal data in its possession or under its control by taking "reasonable security steps or arrangements" to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.[49] In determining whether disclosure of an individual's data to a third party is acceptable, regard is also given to whether a "reasonable person" would consider it appropriate in the circumstances.[50] Professor Chesterman argues that on a whole, the purpose of the *PDPA* appears focused on the management of information, rather than to protect an individual's rights to privacy.[51]

The common law *Tournier* banking secrecy regime, the banking secrecy provisions in the *Banking Act*, and *PDPA*'s data protection provisions can be framed as duty–based frameworks which primarily impose obligations on banks in relation to a customer's data. These provisions set the parameters of a bank's duty and restricts the manner in which a bank is able to share a customer's information. Hence, section 47 of the *Banking Act* is formulated mainly in prohibitive language, i.e. "customer information

[43] *Tournier*, *supra* note 37 at para. 474.
[44] E.P. Ellinger, "Disclosure of Customer Information to a Bank's Own Branches and to Affiliates" (2005) 20:3 Banking and Finance Law Review 137 at 145.
[45] *Ibid.*
[46] *PDPA*, *supra* note 20, s. 2(1).
[47] *Ibid.*
[48] Simon Chesterman, "After Privacy: The Rise of Facebook, the Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012" (2012) Singapore Journal of Legal Studies 391 at 404.
[49] *PDPA*, *supra* note 20, s. 24.
[50] *PDPA*, *supra* note 20, s. 18.
[51] Chesterman, *supra* note 48 at 404.

shall not, in any way, be disclosed by a bank." Likewise, the first limb of section 13 of the *PDPA* states "an organisation shall not … collect, use or disclose personal data about an individual unless…" While safeguarding customer information is still of relevance, open banking is concerned with increased data sharing, and how customers can use and disclose their data held with banks to third parties in order for customers to reap maximum benefit. Open banking shifts the focus away from a bank's duty to safeguard customer information, to a customer's right to share his or her information.

(b) Type of Data

The common law *Tournier* regime takes a broad—brush approach in identifying the type of data that should be subject to banking secrecy. In *Tournier*, it was held that a bank's duty of secrecy extends to "all information derived from account transactions", and it has been argued that it should extend to information gathered from "any aspect of the bank–customer relationship."[52] Similarly, banking secrecy regulations under the *Banking Act* applies to "customer information," which is defined at section 40(A) as deposit information or information relating to a customer's bank account, whether in respect of a loan, investment or other transaction, but does not include information not referable to any named customer or group of named customers. In *PSA Corp. Ltd. v Korea Exchange Bank*, Woo Bih Li JC held that "information" includes any information relating to the account of a customer.[53] In other words, "information" includes any data relating to the customer's account, be it documentary or of another nature, and it is not confined to the details such as the amount held in the account.[54] As stated in section 40(A), information that cannot identify customers is not information for the purposes of section 47(1). Hence, in *Teo Wai Cheong v. Crédit Industriel et Commercial*, the Court of Appeal held that the disclosure of telephone conversations with customers identified as A, B or C was not prohibited.[55] Thus, in general the category of customer data that the *Banking Act* is concerned with is account data that can be linked to individual customers.

Personal data that is subject to data protection provisions is defined in the *PDPA* as "data, whether true or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access."[56] The *PDPA* is wider than the *Banking Act* in that it applies to any data, while the *Banking Act* applies to information relating to a customer's bank account. On the other end, the *PDPA* is narrower in that it protects only natural persons, whether living or deceased, while section 47 of the *Banking Act* applies also to customers that are corporations. In other words, there are partial overlaps between section 47 of the *Banking Act* and the *PDPA*. Section 47 is concerned with a bank customer's financial information while the *PDPA* is concerned with data more broadly. For example, an individual customer's date of birth may be protected by the *PDPA*, it would not be covered by section 47 of the *Banking Act*. However, in totality the *PDPA* and the *Banking Act* take a similar approach in distinguishing what data falls under its regulatory ambit, and both are broadly concerned with whether an individual can be identified from such data.

In contrast, open banking considers very specific categories of data, which overlaps only partially with the data regulated under *Tournier,* the *Banking Act* and the *PDPA*. Australia's Farrell Report has identified four categories of data that may be relevant for open banking:

(i) customer–provided data i.e. information provided directly by customers to their banking institution, for example a customer's personal address and contact details information on their financial situation provided when opening an account or applying for a loan, and information that has been provided for the purpose of making payments, such as payee lists;

---

[52] Alan Tyree, *Banking Law in Australia*, 9th ed. (New South Wales, Australia: LexisNexis Butterworths, 2017) at 205.
[53] *PSA Corp. Ltd. v. Korea Exchange Bank*, [2002] 3 S.L.R. 37 at para. 25. Woo JC was commenting on the equivalent provision in the 1999 revised edition of the *Banking Act*.
[54] Ellinger, *supra* note 44 at 141.
[55] *Teo Wai Cheong v. Crédit Industriel et Commercial*, [2011] SGCA 13 at para. 23.
[56] *PDPA*, *supra* note 20, s. 2(1).

(ii) transaction data i.e. data that is generated as a result of transactions made on a customer's account or service, for example records of deposits, withdrawals, transfers and other transactions undertaken by a customer (such as direct transactions with merchants), account balances, interest earned or charged, and other fees and charges incurred by the customer;

(iii) value–added customer data i.e. data that results from effort by a data holder to gain insights about a customer, for example data from income/assets checks, customer identity verification checks, credit reporting data, credit scores, data on an individual customer that has been aggregated across the customer's accounts, and standardized, cleansed or reformatted to make it more usable; and

(iv) aggregated data sets which are created when banks use multiple customers' data to produce de–identified, collective or averaged data across customer groups or subsets, for example average account balances grouped by postcode or income quintile, or average size of small business overdrafts grouped by industry. [57]

In addition, distinctions are also drawn between data from different accounts such as a customer's deposit, transaction or mortgage accounts.[58] Given the specific categories of data that open banking considers, such as those identified in the Farrell Report, it is critical to identify categories of data with more precision and to draw finer distinctions than those drawn in *Tournier,* by the *Banking Act* or the *PDPA*. Relying on pre–existing definitions of "customer information" or "personal data" in banking secrecy laws or the *PDPA* would be too broad–brush an approach for banks to determine what categories of data can be disclosed pursuant to open banking.

(c) Information Sharing

The exceptions to a bank's duty of secrecy under *Tournier* and the *Banking Act* are arguably ill–suited to facilitate the sharing of information for the use of open banking. As stated, the exceptions to the common law *Tournier* duty of secrecy include where disclosure is required by law or necessary for the fulfilment of a public duty, with the customer's express or implied consent or where it is in the interests of the bank. These exceptions are broadly reflected in the Third Schedule of the *Banking Act*. For example, the Third Schedule specifies that disclosure is permitted where it is necessary for complying with a court order or for the purposes of investigation or prosecution (i.e. required by law).[59] Under the Third Schedule of the *Banking Act*, the two main exceptions to banking secrecy that facilitate the disclosure of customer information to third parties in the ordinary course of conducting one's banking business also mirror the "express or implied consent" and "interests of the bank" exceptions in *Tournier*. Firstly, where disclosure is permitted in writing by the customer (the "**written consent exception**").[60] Secondly, where disclosure of customer information is made "solely in connection with the performance of operational functions of the bank where such operational functions have been outsourced" (the "**outsourcing exception**").[61] As this discussion will show, neither the *Tournier* nor the *Banking Act* exceptions are particularly well–suited for an open banking model.

In the open banking paradigm, holders of banking data securely share a customer's banking data at the customer's direction, with parties nominated by the customer, in a form that facilitates its use.[62] Critically, it is the customer that initiates the information sharing process. Hence open banking provides for the seamless transfer of customer information to nominated parties, and the customer does not need

[57] The Treasury, *supra* note 3 at 33-34.
[58] For example, the CDR imposes different timelines on Australia's Big Four Banks regarding data from a customer's deposit and transaction accounts (mandatory access by February 2020), and data from mortgage accounts (mandatory access after February 2020). See The Treasury, *supra* note 31.
[59] *Banking Act, supra* note 19, Third Schedule, Part I at para. 5.
[60] *Banking Act*, *supra* note 19, Third Schedule, Part I at para. 1.
[61] *Banking Act*, *supra* note 19, Third Schedule, Part II at para. 3. See also Singapore, Monetary Authority of Singapore, *Notice 634 Banking Secrecy – Conditions for Outsourcing* (Singapore: Monetary Authority of Singapore, 2004).
[62] The Treasury, *supra* note 3 at 1.

to undertake this process manually. These nominated parties may include competing providers of banking and financial services, providers of comparator services that can identify which banking products and services best meet the customer's needs, or providers of tools that may help a customer better manage their finances or tax affairs.[63] The underlying assumption is that customers will benefit from the ease of switching between financial service providers and from the availability of comparator services. Both are premised on the sharing of customer information in a useful, likely electronic, form that minimizes friction if a customer wants to move to a competing financial service provider or use a comparator service.

While disclosure of customer information is envisaged under *Tournier's* express/implied consent exceptions or the written consent exception, the flavour of such exceptions is permissive (for example, the written consent exception states where "disclosure is *permitted*") and not directive. In other words, while a customer may *permit* the disclosure of his information to a competing provider or to comparator services, the bank is not obliged to entertain such permission or even initiate the process to obtain such permission. In the event that a bank chooses to collaborate with a third party in the spirit of open banking, the identity of the third party is entirely within the bank's prerogative, and the customer's choice would be limited to opting in for such an arrangement. If the customer cannot initiate and direct the information sharing process, and without information sharing occurring directly between institutions in a form that facilitates its use, the benefits of open banking cannot be realized. It is also unlikely that the release of customer data to competing providers or to comparator services, as envisaged by open banking, would fall under the *Tournier* exception where it is in the interest of the bank, or under the outsourcing exception. The sharing of customer information with competing providers of financial services is unlikely to be in a bank's interest. Also, the very definition of an outsourcing arrangement, i.e. for a service provider to "provide *to the bank* any service that is currently or is commonly performed by the bank; or provide any service to the public *in the name of the bank*"[64] is targeted at enabling the bank to streamline its operations, for example in claims administration and document processing[65] and not to widen customer choice. Outsourcing is directed at helping banks provide their financial services, and not at helping customers maximize the benefits of available financial services.

(d) A Strain on Existing Frameworks

To conclude this section, while *Tournier* and existing legislative frameworks governing banking data have been useful in facilitating bank–customer relations, these may be challenged with the onset of open banking. This is because open banking does not start from the position of restricting the flow of customer information to within the individual bank, but is instead focused on sharing customer information with other entities. In the open banking model, there is also increasing emphasis on whether customers can *control* the flow of their data even after they have given their consent for disclosure. Hence the discussion extends beyond a bank's duty of secrecy as an incident of the law of agency. The focus is, rather, on how a customer can direct the use of his/her banking data in a manner that will maximize benefits accruing to them, such as by tapping on services provided by non–traditional financial services providers. While the confidentiality of customer information is still relevant, the focus has shifted to how a customer is able to control and therefore maximize the beneficial use of his/her banking data. Within the open banking paradigm, a customer's banking data is no longer envisaged as a mere by–product of using banking services, but instead as a valuable resource that can be used by the customer. It is with this observation that the article turns to consider whether property law concepts of ownership can be useful in framing the flow of banking data in an open banking paradigm.

---

[63] *Ibid*.
[64] See Singapore, Monetary Authority of Singapore, *Section 58A of the Banking Act: Regulation of outsourcing arrangement* (Singapore: Monetary Authority of Singapore, 2019), online: <https://www.mas.gov.sg/-/media/Annex-C--Draft-Amendments-to-the-Banking-Act--Section-58A.pdf>.
[65] Examples of outsourcing arrangements are listed at Singapore, Monetary Authority of Singapore, *Guidelines on Outsourcing (with effect from 8 October 2018)* (Singapore: Monetary Authority of Singapore, 2018).

4. OPEN BANKING AND DATA OWNERSHIP

Data ownership is a fundamental issue for open banking because open banking is predicated on the view that banking data belongs to the customer and the customer should be able to control how it is used and with whom it is shared.[66] Data ownership may encompass issues such as what data rightfully belongs to the customer and whether data concerning customers generated by banks is the bank's proprietary information.[67] Colloquially, the language of ownership may also be used in reference to data such as contact numbers and residential addresses which raises the question whether such data *belongs* to an organisation's customers.[68] However, the concept of ownership sits uneasily with data. While data may be characterized as an asset, arguably the most valuable asset of the 21st century,[69] there is difficulty in characterizing data as property that is capable of ownership. The legal orthodoxy in common law jurisdictions is that information, or data, in itself is not property.[70] Information may give rise to intellectual property rights but the law has been reluctant to treat information itself as property.[71] When information is created and recorded for example to constitute an electronic database, there is a distinction between the information itself, the physical medium on which it is recorded (such as a disk) and the rights (such as database right and copyright) to which the information gives rise.[72] Whilst the physical medium and intellectual property rights are treated as property, the information itself is not.[73] The reality is that property law struggles to accommodate data ownership.[74]

Hence, legislative action has been taken in some jurisdictions to accord ownership rights to data. Australia's CDR aims to create ownership rights over data across different sectors, with the banking sector designated as the first use–case. Such data rights provide consumers with the ability to efficiently and conveniently access specified data held about them by businesses (data holders), and to authorize the secure disclosure of that data to accredited data recipients or to themselves.[75] The CDR is designed to give consumers more control over their data, leading to greater choice in where they take their business.[76] The control a customer has over his/her banking data is critical in an open banking paradigm given that it is purportedly a customer–centric development that allows customers to reap maximum benefits from their data. Logically, this is premised on a customer's ability to first exercise ownership rights over their own data.

This section evaluates how ownership rights can be accorded to data. First, this section evaluates the extent to which a duty–based framework, such as that found in *Tournier*, Singapore's *Banking Act*, and Singapore's *PDPA*, can accommodate data ownership using the taxonomy of ownership developed by

---

[66] Black & Koskivirta, *supra* note 10 at 39.
[67] See, for example, questions of data ownership raised in Monetary Authority of Singapore, "The Future of Banking – Evolution, Revolution or a Big Bang?" (16 April 2018), online: *Monetary Authority of Singapore* <https://www.mas.gov.sg/news/speeches/2018/the-future-of-banking>.
[68] *COURTS (Singapore) Pte. Ltd.*, [2019] S.G.P.D.P.C. 4 at para. 6.
[69] European Consumer Commission, Meglena Kuneva, *Personal Data is the New Oil of the Internet and the New Currency of the Digital World* (Keynote Speech at the Roundtable on Online Data Collection, Targeting and Profiling, SPEECH/09/156, 31 March 2009).
[70] See, for example, dicta in *Clearlab SG Pte. Ltd. v. Ting Chong Chai and Others*, [2015] 1 S.L.R. 163 at para. 85 and *Your Response Limited v. Datateam Business Media Limited*, [2014] E.W.C.A. Civ. 281 at para. 42 [*Your Response Limited*].
[71] *Your Response Limited*, *supra* note 70 at para. 42.
[72] *Ibid.*
[73] *Ibid.*
[74] See dicta by the English Court of Appeal in *Fairstar Heavy Transport NV v. Adkins*, [2013] Civ. 886 at para. 47: a claim to property in intangible information presents obvious definitional difficulties, having regard to the criteria of certainty, exclusivity, control and assignability that normally characterize property rights and distinguish them from personal rights.
[75] See Australia, Commonwealth, Australian Competition & Consumer Protection Commission, *Explanatory Statement – Proposed Competition and Consumer (Consumer Data Right) Rules 2019* (Canberra, Australia: Australian Competition & Consumer Protection Commission, 2019) at para. 2, online: <https://www.accc.gov.au/system/files/Proposed%20CDR%20rules%20-%20Explanatory%20Statement%20-%20August%202019.pdf >.
[76] *Ibid.*

Anthony Honoré, the pre–eminent property–rights scholar. Where applicable, this section draws a comparison with the rights–based approach taken by Australia's proposed CDR. Honoré identifies eleven standard incidents of the "liberal concept of full individual ownership" which are constitutive of the concept of ownership.[77] These are: the right to possess (i.e. to have control over the object); the right to use (i.e. to exercise personal use of the object); the right to manage or control (i.e. to determine how and by whom the object is used); the right to income or profit (i.e. to derive a benefit from the use of the object); the right to capital (i.e. the power to alienate and liberty to consume the object); the right to security (i.e. that the person will remain owner of the object); the rights of transmissibility or transfer (i.e. the ability to transfer the rights of ownership to another); the rights to absence of term (i.e. the presumption of indeterminate length of ownership); the owner's duty to prevent harm (i.e. to prevent the use of the object in harmful ways); the liability to execution (i.e. the liability to have the object or asset seized in payment of a debt); and the incident of residuarity (i.e. rights may expire or be abandoned so as to vest in someone else).[78] The first eight incidents will be discussed in turn. The remaining three incidents, being the owner's duty to prevent harm, liability to execution and incident of residuarity, will not be discussed in this article given their limited application to how a customer might interact with its banking data in an open banking model. This section does not consider the normative question of whether data should be subject to property rights, a separate debate that has generated significant academic discussion with divergent views.[79]

(a) Rights to Possess (or Access) and Use

While the right to possess is generally concerned with tangible things, it may be more appropriate to speak of access to data, an intangible. Logically, discussion of access rights must necessarily predicate the issue of use. Under the *Banking Act*, customers do not have any statutory right to request for data that the bank holds on them. Likewise, in *Tournier* the focus is on a bank's duty of secrecy and the exceptions to such a duty, but not on how customers are able to access information on them held by banks. The customer's right to request for the release of account information is largely determined by the standard terms and conditions governing bank accounts. A survey of the standard terms and conditions governing the provision of account statements to customers across seven major commercial banks in Singapore[80] shows that the frequency in which such statements are sent is entirely up to the bank's discretion. Other than the provision of account statements, there is little reference to the provision of other forms of data. This is problematic given that open banking envisages the sharing of data, such as value–added customer data referred to above, that may not be accessible to the customer through account statements. Only one bank specifies that it "may also make available for viewing online a record of the transactions performed in respect of such account during a specified period"[81] subject to the bank's own terms and conditions. Hence, customers largely do not seem to have an express contractual right to access data concerning their own transaction history.

While bank customers may be able to access their transaction history on a mobile or internet banking service, the terms and conditions governing the use of such services across the seven major commercial banks in Singapore generally caveats a customer's access to his or her information on such platforms. For example, one set of terms states that if a customer does not allow the bank to share information

---

[77] Tony Honoré, *Making Law Bind: Essays Legal and Philosophical* (Oxford: Clarendon Press, 1987) at 162.
[78] *Ibid.*
[79] See, for example, Lothar Determann, "No One Owns Data" (2018) 70:1 Hastings Law Journal 1–44; Christopher Rees, "Who owns our data?" (2014) 30 Computer Law & Security Review 75–79; and
Andreas Boerding, Nicolai Culik & Christian Doepke et al., "Data Ownership—A Property Rights Approach from a European Perspective" (2018) 11:2 Journal of Civil Law Studies 325–346.
[80] Namely, DBS Bank, OCBC Bank, United Overseas Bank, Citibank Singapore, HSBC Bank (Singapore), Maybank Singapore Limited & Standard Chartered Singapore.
[81] See clause 9 of "Terms & Conditions Governing Deposit Accounts" *OCBC Bank* (2019), online: <https://www.ocbc.com/personal-banking/accounts/terms-and-conditions-governing-deposit-accounts.html>.

relating to his/her money and electronic account with the bank's trusted third–parties,[82] the bank may not be able to continue providing its electronic services to the customer.[83] On that same bank's mobile phone banking application, it is stated that a customer may view his or her transaction history for a savings or current account for a maximum six month period. In totality, customers have limited rights to access the information[84] banks hold on them under their account contract.[85] While customers may obtain printed account statements, in certain instances upon paying a retrieval fee, there is no contractual provision for obtaining such data in an electronic form. The inability to obtain one's data in an electronic form poses difficulties for data portability, which is essential for open banking. Customers may not be able to electronically share their data with, and hence utilize financial services provided by other service providers. Thus, it is difficult to conclude that customers have an absolute right to "use" their banking data for their own means. Indeed, it is often banks who will utilize such data for their own purposes set out in their privacy policies. One such privacy policy cites uses such as for general support, internal operations including research and analysis, compliance and seeking legal advice, and marketing purposes.[86]

Under the *PDPA*, individuals are able to request access to their personal data that the organisation has collected.[87] However, the Fifth Schedule provides carve–outs to an individual's right to request access. The Fifth Schedule expressly excludes, *inter alia,* any request for data that would "unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests; [where] the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; … [where] information that is trivial." These carve outs effectively endow organisations with a wide discretion to reject an individual's request for data. For example, it is unclear if a customer asking for transaction data since the start of his account opening would constitute a request where "the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests." The charges imposed by banks for the retrieval of monthly statements[88] dating back beyond the month preceding the request is an indicator that banks generally view these requests as burdensome. Essentially, individuals are required to pay a fee before their requests can be fulfilled. It is also unclear whether the standard of triviality is an objective one, given that it is unlikely that an individual requesting for such information would himself deem it trivial. Consequently, it would be difficult to conclude that individuals have any rights to access their data under the *PDPA*.

In contrast, the CDR specifically legislates a right to access data. There are three types of CDR data requests that can be made, namely product data requests made by any person, consumer data requests made by CDR consumers, and consumer data requests made on behalf of CDR consumers by accredited

---

[82] See "Terms & Conditions Governing Electronic Services" *DBS Bank* (2019), online: <https://www.dbs.com.sg/personal/deposits/terms-conditions-electronic-services.page>. Clause 11.5 states that DBS Bank reserves the right to use any provider, subcontractors and/or agents on such terms as they deem appropriate.

[83] *Ibid.* at clause 10.4.

[84] For example, general categories of such information may include information on a customer's particulars, money, account, electronic instructions, or relevant particulars of an authorized user.

[85] Graham Greenleaf & Alan Tyree, "Bankers' Duties and Data Privacy Principles: Global Trends and Asia-Pacific Comparisons" in Sandra Booysen & Dora Neo, eds., *Can Banks Still Keep A Secret? - Bank Secrecy in Financial Centres Around the World* (Cambridge, UK: Cambridge University Press, 2017) 31 at 58.

[86] See "DBS Bank Privacy Policy" *DBS Bank* (2019), online: <https://www.dbs.com/privacy/policy/default.page>.

[87] *PDPA, supra* note 20, s. 21.

[88] Including statement of accounts, time deposit interest statements and advices, deposit/withdrawal/debit/credit vouchers and savings account details. See, for example, "OCBC Bank's Fees & Charges Guide for Personal Banking Products" *OCBC Bank* (2019) online: <https://www.ocbc.com/assets/pdf/pricing%20guides/personal%20banking%20pricing%20guide.pdf>.

data recipients.[89] An eligible CDR consumer[90] may therefore request that a data holder, i.e. a business that collects and stores information on CDR consumers, disclose some or all of their CDR data. CDR data is information that falls within, or is wholly or partly derived from a class of information specified in the instrument designating the banking sector under Australia's Competition and Consumer Act 2010.[91] Notably, the data holder cannot charge a fee for the disclosure of the required consumer data.[92] Furthermore, to facilitate access, such data is required to be shared in a human–readable form as opposed to machine–readable.[93] No restrictions are to be placed on the customer as to what he/she chooses to do with such information.[94] The CDR operates in addition to existing data sharing arrangements and practices. In the banking sector, this means that the CDR operates in addition to the mechanisms by which banks currently provide information to their customers, such as through bank statements that are available online, for download.[95] In this manner, individuals are accorded an ownership right of access in relation to their data held with banks.

(b) Right of Control

In a model that envisages increased sharing of customer banking data, the question of control is generally the *leitmotif* of open banking.[96] While possession is concerned with the physical control of tangible objects; practical control is a broader concept, capable of extending to intangible assets.[97] There is no concept of having "control" over one's banking data in Singapore's *Banking Act* or under the common law set out in *Tournier*. Both systems recognize that a customer may consent to the bank disseminating his/her information to a third party by giving permission. It has been argued that the primary idea behind the consent exception is that it serves to cover instances of disclosure that the customer desires in his/her own interests.[98] It is a cooperative exception to a bank customer's right to privacy and means that permission is knowingly given and with a known disclosure in mind.[99] However, it has been observed that in practice, there is a qualitative difference between objective or formal consent as contained in a bank's terms and conditions (which is how consent is usually obtained in Singapore) and genuine, subjective consent.[100] Formal consent is arguably artificial as it is given in advance and in a vacuum, and the customer does not have any particular instance in mind in which he or she is waiving his or her right to privacy.[101] Where a customer has consented to the disclosure of his or her information, it may be insufficient to justify all instances of disclosure. For example, notwithstanding that customer consent for onward disclosure of information has been obtained, the MAS imposes additional requirements on banks to discharge their standard of care when disclosing such information in the course of outsourcing arrangements.[102] Arguably, such an approach implicitly recognizes the limitations of obtaining formal, prior consent from customers. Furthermore, there are numerus instances under the Third Schedule to the *Banking Act* pursuant to which disclosure is possible without the consent of the

---

[89] Australian Competition & Consumer Protection Commission, *supra* note 75 at para. 1.22.
[90] A CDR consumer for the banking sector is eligible if he/she is 18 years or older and has an account with the data holder that is an open account and set up in such a way that it can be accessed online. See Australian Competition & Consumer Protection Commission, *supra* note 75 at para. 1.27.
[91] *Competition and Consumer Act 2010*, *supra* note 29, s. 56AI(1).
[92] *Competition and Consumer Act 2010*, *supra* note 29, s. 56BU.
[93] Australian Competition & Consumer Protection Commission, *supra* note 75 at para. 1.62.
[94] *Ibid.* at para. 1.63.
[95] *Ibid.* at para. 1.3.
[96] Black & Koskivirta, *supra* note 10 at 39.
[97] *Your Response Limited*, *supra* note 70 at para. 23.
[98] Sandra Booysen, "Singapore" in Sandra Booysen & Dora Neo, eds., *Can Banks Still Keep A Secret? - Bank Secrecy in Financial Centres Around the World* (Cambridge, UK: Cambridge University Press, 2017) 278 at 291. Dr. Booysen was specifically addressing the written permission exception in Singapore's Banking Act but the reasoning seems to be equally applicable to the common law consent exception.
[99] *Ibid.*
[100] Sandra Booysen, "Bank Secrecy in Singapore and Customer's Consent for Disclosure" (2011) 26:10 Journal of International Banking Law & Regulation 501 at 504.
[101] *Ibid.*
[102] Singapore, Monetary Authority of Singapore, *Outsourcing by Banks and Merchant Banks (Consultation Paper P002-2019)* (Singapore: Monetary Authority of Singapore, 2019) at para. 4.5.

customer. In totality, it is difficult to conclude that *Tournier* or Singapore's *Banking Act* give customers a "right of control" over their banking data.

While there is no concept of control in Singapore's *PDPA*, the meaning of control in the context of data protection has been held by the Singapore Personal Data Protection Commission as generally to cover the ability, right or authority to determine the purposes for and/or the manner in which, personal data is processed, collected, used or disclosed.[103] In *AIG Asia Pacific Insurance Pte. Ltd.*, it was held that the organisation which engages a data intermediary to process personal data on its behalf will "always have overall control of the purposes for which, and manner in which, personal data is processed, collected, used or disclosed."[104] Notably, possession is distinct from control. Where an organisation transfers personal data to its data intermediary, the organisation could remain in control of the personal data set while, simultaneously, the data intermediary may have possession of the same personal data set.[105] Hence, it would appear that control of an individual's data, as long as it has been collected by an organisation, ultimately lies with the organisation in charge of such collection even if there is subsequent third party involvement. Thus, an individual would not have any meaningful "right of control," or power to direct how he/she would like his/her data to be released to other organisations as envisaged by the open banking paradigm.

Australia's CDR attempts to bolster a customer's right of control over his/her data by having an accreditation regime. The accreditation regime sets standards for an accredited person[106] to meet before it can receive customer data from a data holder (such as a bank). An entity that requires accreditation are persons who are not authorized deposit–taking institutions such as a non–bank lender offering personal loans.[107] Under the accreditation regime, standards include ongoing reporting obligations,[108] adequate privacy safeguards to protect CDR data from misuse, interference, loss, unauthorized access, modification or disclosure,[109] and an obligation to destroy or de–identify redundant CDR data.[110] Critically, accreditation is a necessary pre–condition for a third–party entity to receive CDR data. When a consumer requests that an accredited person provides them with goods or services that require the use of their CDR data, the accredited person may then make a request to the data holder for such data. The consumer must consent to the accredited person collecting and using their data to provide the specified goods or services in order for the request to be valid.[111] Thus, the accreditation regime ensures that the customer has oversight over the sharing of his/her data between a data holder and an accredited person. However, this oversight does not extend to outsourcing arrangements that a data holder may contractually enter into with another person, although such persons are subjected to limits on the utilisation of a customer's CDR data.[112]

(c) Rights to Security, Transfer and Absence of Term

Given that the rights to security (i.e. that the person will remain owner of the object) and the right to absence of term (i.e. the presumption of indeterminate length of ownership) are two sides of the same coin, they will be considered here in tandem. A customer's right of security is reflected in the *Tournier* express/implied consent exceptions and the *Banking Act* consent requirements where an individual's consent is generally required before the bank discloses his/her personal information to other entities. However, as noted, in practice the way in which banks obtain consent does not necessarily constitute

[103] *AIG Asia Pacific Insurance Pte. Ltd.*, [2018] S.G.P.D.P.C. 8 at para. 18.
[104] *Ibid.* at para. 19.
[105] *Re The Cellar Door Pte Ltd and Another*, [2016] S.G.P.D.P.C. 22 at para. 17.
[106] See *Competition and Consumer Act 2010*, *supra* note 29, s. 56CA(1).
[107] Australian Competition & Consumer Protection Commission, *supra* note 75 at para. 1.132, example 11.
[108] Australian Competition & Consumer Protection Commission, *supra* note 32, Rules 5.9, 9.3(2) & Schedule 1.
[109] *Competition and Consumer Act 2010*, *supra* note 29, s. 56EO(1). See also Australian Competition & Consumer Protection Commission, *supra* note 28, Schedule 2.
[110] *Competition and Consumer Act 2010*, *supra* note 29, s. 56EO(2).
[111] Australian Competition & Consumer Protection Commission, *supra* note 75 at para. 1.71.
[112] Australian Competition & Consumer Protection Commission, *supra* note 32, Rule 1.10.

genuine, subjective consent and customers are accordingly not aware of the exact manner and purposes for which their data could be utilized. If such consent is valid, once a customer has given consent, the exact use of their data by the bank is beyond his/her purview. Furthermore, where an individual generates data through the use of a banking service, for example by generating spending patterns through the use of an online banking service, it becomes ambiguous as to whether there is a right to security or absence of term over such data. For example, from a survey of the standard terms and conditions of personal deposit accounts across seven major commercial banks in Singapore,[113] the clauses governing "closure of accounts" are silent as to what happens to a customer's banking data once the bank account has been closed. It is unlikely that customers will have continued access to the entirety of their data (such as transaction history generated by the use of an online banking platform) apart from any printed bank statements they may possess, given that their security credentials may be invalidated with the closing of their accounts. Hence, there is arguably no long–term right to security and absence of term over one's banking data encapsulated in *Tournier* or Singapore's *Banking Act*. In contrast, individuals have some rights of security and absence of term over their own data under Singapore's *PDPA* given that they are generally not subject to any limitations in the use or disclosure of their own data, unlike organisations which are subject to the principle of finality and hence limited in their re–use of collected information.[114]

Australia's CDR attempts to accord a right to security to consumers over their banking data by introducing provisions on the deletion of redundant data. Under the CDR, consumers who have given their consent to an accredited person to collect and use their data may elect for their collected data, and any data derived from it, to be deleted when it becomes redundant.[115] The CDR defines "redundant data" as having the meaning given by section 56EO(2)(a) of the Competition and Consumer Act 2010.[116] Section 56EO(2)(a) in turn states that "redundant data" is data that is no longer needed for a purpose permitted under the CDR. Critically, a consumer is free to make this election when giving consent or at any other time before the expiry of their consent.[117] Such provisions appear to facilitate rights to security as a consumer has the discretion to actively direct that copies of his/her data be removed. This goes a step further than simply revoking one's consent as it addresses the existence of data that has already been collected. However, such a right to security under the CDR is not absolute. Consumers must exercise this election before his/her consent has expired. Hence, in the scenario where a consumer closes his/her bank account (and arguably terminates any contractual consent given to the bank with the end of the bank–customer relationship), it is still unclear what happens to the customer's banking data held with the bank.

The right of transfer (i.e. the ability to transfer the rights of ownership to another) is arguably evident through Singapore's *Banking Act* requirement of obtaining customer consent for disclosure of information to third parties. However, it is possible that once individuals have consented pursuant to a widely worded clause in their contract, they relinquish any ability to influence the use of their own data as it is governed by the bank's standard terms and conditions and is within the bank's prerogative. In a case decided by the Office of the Canadian Privacy Commissioner,[118] the complainant held a credit card account with Bank A and had objected to the transfer of his account information to Bank B, who had acquired Bank A's card program. The complainant was of the view that Bank A should have obtained his express consent for the sale of his personal information to Bank B. The Privacy Commissioner

---

[113] Namely, DBS Bank, OCBC Bank, United Overseas Bank, Citibank Singapore, HSBC Bank (Singapore), Maybank Singapore Limited & Standard Chartered Singapore.
[114] *PDPA, supra* note 20, s. 18.
[115] Australian Competition & Consumer Protection Commission, *supra* note 32, Rule 4.11(1)(e).
[116] Australian Competition & Consumer Protection Commission, *supra* note 32, Rule 1.7(1).
[117] Australian Competition & Consumer Protection Commission, *supra* note 32, Rule 4.16(1).
[118] "Customers allege that sale of personal information by one bank to another occurred without knowledge and consent: PIPEDA Case Summary #2006-350" *Office of the Privacy Commissioner of Canada*, online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-350/>.

dismissed the complaint and held that Bank A was entitled to assign the complainant's personal information to Bank B as it had previously issued a revised cardholder agreement to the complainant which contained an assignment clause. The assignment clause indicated that the bank may transfer by way of assignment, sale or otherwise, any or all its rights under the agreement. The broad consent to disclosure clauses used by banks in Singapore have yet to be tested in court. As indicated earlier, there are different views as to whether such clauses are compatible with section 47 of the *Banking Act*. If they are indeed valid, the position in Singapore would be similar to that in Canada and once an individual has consented to the use and disclosure of his/her account information, it is within the bank's discretion to contract with other banks or organisations to transfer such data. Hence, while an individual may have a right of transfer, the degree of "ownership" it accords is limited given that the individual is removed from the decision–making process concerning the onward transmission of his/her data to a third–party organisation. In contrast, the CDR attempts to address this issue through the accreditation regime as discussed above.

(d) Rights to Income and Capital

Tournier, the *Banking Act*, and the *PDPA* does not explicitly address the economic dimension of data and these categories of ownership rights must therefore be examined from first principles. A starting point would be to recognize the economic value of data. The Australian Banking Association has reiterated its belief that the open data economy should recognize the economic value of data.[119] For example, personal data allows for the prediction of many aspects of a person's actions, such as where that person prefers to go or what that person prefers to eat.[120] This then translates into targeted marketing by banks and other businesses. Antitrust scholars have argued for the treatment of data as a product, since information and data while different from traditional goods and services, pose problems familiar to competition and antitrust law such as monopolistic behaviour and collusion.[121] The value of data lies in the predictability it provides in ascertaining demand before developing a product, whether financial or otherwise. Across industries and business functions, data is now recognized as an important factor of production.[122]

Regarding the right to capital (i.e. the power to alienate and the liberty to consume the object), it is arguable that the common law *Tournier* regime of banking secrecy, the *Banking Act*, and the *PDPA* equip individuals with the power to alienate others from the use of their personal data through the requirements of obtaining consent before disseminating such information to third parties. The consent regime under the *PDPA* is more rigorous than the *Tournier* express/implied consent exceptions and the Written Consent Exception found in the *Banking Act* in the sense that the *PDPA* recognizes actual consent only if the individual has been informed as to the purpose for which the personal data is being collected, used or disclosed.[123] Hence, it is possible for an individual to prevent organisations from accessing his/her data by withholding consent for such data to be collected, used or disclosed. However, the *PDPA* recognizes deemed consent as well, which refers to circumstances in which an individual, without expressly giving consent, voluntarily provides the personal data and it is reasonable that he or she *would* provide the data.[124] In this instance, the power of alienation is significantly weakened given that an individual, without giving express consent, may be deemed through his/her actions (whether having applied his/her mind to the consequences of such actions or otherwise) to have consented to the collection, use or disclosure of his/her data.

---

[119] Pip Freebairn, *Response to the Farrell Report into Open Banking* (New South Wales, Australia: Australian Banking Association, 2018) at 6.
[120] Determann, *supra* note 80 at 38.
[121] Mark R. Patterson, *Antitrust Law in the New Economy: Google, Yelp, LIBOR, and the Control of Information* (Cambridge, Massachusetts, US: Harvard University Press, 2017) at 173–179.
[122] James Manyika, Jacques Bughin & Michael Chui et al., *Big data: The next frontier for innovation, competition, and productivity* (McKinsey Global Institute, 2018) at 3.
[123] *PDPA, supra* note 20, ss. 14(1)(a) & 20.
[124] *PDPA, supra* note 20, ss. 15(1).

Regarding the right to income (i.e. to derive a benefit from the use of the object), the *Tournier* exceptions, the *Banking Act*, and *PDPA* facilitates an individual's ability to benefit from the use of their data by providing a framework governing the flow of data in a bank–customer relationship, or between an organisation and an individual. However these benefits primarily constitute services, such as a banking service, provided by the organisation to which an individual has disclosed his/her data. The economic dimension to any potential benefits is not addressed. Admittedly, Honoré's taxonomy does not specify that a benefit derived from the use of an object must be economic in nature. However, it is pertinent to consider an individual's ability to derive economic benefit from the use of their data given the unprecedented economic value creation that data presents in a digitalized economy.[125] In this vein, an organisation's ability to derive economic benefit from individual data appears to far outweigh the individual's ability to do so. For example, an individual would have to pay a monetary fee, in addition to providing his/her data, in order to obtain a banking service such as the use of a credit card. Yet organisations are able to collect and use this data to support individualized service–delivery business models that can be monetized.[126] Instead, individuals may suffer economic detriment in the form of price discrimination from organisations that use information on customers to price products at the amount that individual would pay.[127] Price discrimination arises because customers do not pay a uniform price for a product, but are charged differently based on their own purchase history. Traditionally, sellers had much less information about their consumers than is now available, a predicament that forced sellers, at least in some instances, to set terms that were more favourable than needed to attract buyers.[128] However, now to the extent that sellers have access to more personal information of consumers, this advantage to consumers could disappear.[129] In short, individuals do not appear to have the right to capital or the right to income in relation to their own data in a way that recognizes the economic dimension of data.

While Australia's CDR does not explicitly accord any rights to income and capital over banking data to customers, it makes a first step in recognising that data carries economic value. In particular, the CDR prohibits an accredited person from requesting consent from consumers to use or disclose their data for the purpose of selling it, unless such data can no longer be traced back to the consumer.[130] In addition, the data holder (such as the bank) is also prohibited from obtaining consent to use a customer's data, including the aggregation of such data, for the purpose of identifying, compiling insights in relation to, or building a profile in relation to a third party.[131] Hence the CDR recognizes that a customer's banking data, including data generated through the use of a bank's services, carries economic value by facilitating other entities' ability to price a product or service more accurately. The CDR restrictions on seeking customer's consent arguably gives a customer a partial, negative right to income and capital, by having the ability to deny third party entities (although there are no restrictions imposed on the data holder itself) the opportunity to profit from such data.

5. CONCLUSION

While one may use terminology alluding to the ownership of data, provisions found in Singapore's banking secrecy or data protection regulations have few genuine incidences of ownership. A similar statement is appropriate also for jurisdictions having the *Tournier* regime of bank secrecy. This is problematic given that the issue of ownership and control is fundamental to the development of open

[125] Geneva, Switzerland, World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (Geneva, Switzerland: World Economic Forum, 2011) at 5.
[126] *Ibid.*
[127] Mark R. Patterson, *supra* note 122 at 174.
[128] *Ibid.*
[129] See, for example, Anna Bernasek & D. T. Mongan, *All You Can Pay: How Companies Use Our Data to Empty Our Wallets* (New York: Nation Books, 2015).
[130] Australian Competition & Consumer Protection Commission, *supra* note 32, Rule 4.12(3)(a).
[131] Australian Competition & Consumer Protection Commission, *supra* note 32, Rule 4.12(3)(b). See also Australian Competition & Consumer Protection Commission, *supra* note 75 at para. 1.96.

banking. If a customer is able to take "ownership" of his or her own data, then open banking may be conceptualized as a simple exercise of property rights over one's data. Where such property rights do not exist, it is challenging to identify a legal basis for a customer to direct the use of his/her banking data. However, data ownership should not be perfunctorily read into existing legislation. The creation of property rights in data have far reaching implications which should be created only after careful consideration.[132] This is especially so given that conceptualising data as "property" would mean that individual data subjects and owners will be able to exclude others from using or accessing that data.[133] Thus in the absence of express legislation providing for elements of ownership such as those found in Honoré's taxonomy, there exists a legal lacuna concerning how customer data is to be managed within an open banking model.

Open banking raises important questions of ownership and control that cannot answered by recourse to property law concepts but is best addressed by legislation. This is especially pertinent given that data has become an important currency in commerce today.[134] The economic value of data may not be adequately captured in existing legislative frameworks regulating customer banking data. An analogy can be drawn between the existing approach towards regulating customer data that primarily aims to boost customer confidence or to regulate the flow of data, and to traffic laws. Traffic laws that govern when a vehicle has the right of way, may be adequate for improving the confidence of road users in using roads and for regulating the flow of traffic. However, such purely directional laws would be inadequate for regulating activities that carry economic value, such as securities trading on the stock exchange. This is because the movement of securities on the stock exchange has economic ramifications that the flow of traffic does not. Similarly, as customer data becomes an increasingly valuable resource, legislation governing customer data must take its commodity–like characteristic into account. This is critical in protecting customer interests and will build on the spirit of banking secrecy laws, which were first enacted in the customer's interest. Notably, Australia's CDR has identified the banking sector as the first applicable use case for its data ownership provisions because it recognizes that banking law provides a firm foundation for ownership concepts through the duties that a bank owes it customer, including the duty to keep a customer's information confidential.[135] The long–established banker–customer relationship can therefore guide the development of open banking, and once the framework is built, it can be extended to other sectors.[136] The nature of the data economy is such that there can be the potential for a loss in trust in the institutions that govern the market.[137] As a result, the role of governments in legislating, regulating, and overseeing the market for data will increase in importance.[138] In this vein, legislating specific rights suitable for an open banking paradigm, and to bolster a customer's control over his/her banking data may be the best approach.

---

[132] *Your Response Limited*, *supra* note 70 at para. 27.
[133] Determann, *supra* note 79 at 35.
[134] Michelle Evans, "Why Data Is The Most Important Currency Used In Commerce Today" *Forbes* (12 March 2018), online: <https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/>.
[135] The Treasury, *supra* note 3 at v.
[136] *Ibid.*
[137] Sree Kumar, Warren B. Chik & See-Kiong Ng et al., *The Data Economy : Implications from Singapore* (New York, US: Routledge, 2019) at 5.
[138] *Ibid.*