INTERNET POLICY REVIEW
Journal on internet regulation

Volume 14 **Issue** 1

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

The many shades of open banking: A comparative analysis of rationales and models

Giuseppe Colangelo *University of Basilicata* giuseppe.colangelo@unibas.it
Pankhudi Khandelwal *European University Institute*

DOI: https://doi.org/10.14763/2025.1.1821

Published: 22 January 2025
Funding: The authors did not receive any funding for this research.
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Colangelo, G., & Khandelwal, P. (2025). The many shades of open banking: A comparative analysis of rationales and models. *Internet Policy Review*, *14*(1). https://doi.org/10.14763/2025.1.1821

Keywords: Open banking, FinTech, Standards, Data, Regulation

Abstract: Despite its growing success, open banking (OB) struggles to present a coherent identity. Indeed, despite its widespread adoption around the world, various models can be identified based on rationales, the nature of data-sharing obligations, and the standardisation process. Against this background, the paper aims to evaluate the consistency of OB policies. To this end, our analysis adopts a novel approach by examining the primary rationales behind OB regulatory initiatives in some major countries (i.e., the EU, UK, Australia, the US, India, and Singapore). Identifying these rationales is crucial for assessing whether the specific features of OB solutions implemented in each country are aligned with the intended policy goals. Therefore, the paper first identifies the primary rationales supporting OB initiatives in these countries and then examines their data-sharing and standardisation approaches. By mapping the primary rationales and models in terms of data-sharing obligations and standardisation solutions, the comparative analysis shows that variations in models and approaches among the examined jurisdictions do not necessarily reflect differences in the policy goals pursued through the OB regime. As a result, by recommending regulatory and technical solutions that better align with the intended policy goals of an OB regime, such a comparative analysis can assist policymakers in countries considering the introduction of open banking to design a model that best suits their needs.

Introduction

Open banking (OB) is generally defined as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, greater financial transparency options for account holders, marketing, and cross-selling opportunities (Basel Committee on Banking Supervision, 2019).

In recent years, OB has gained increasing attention due to several legislative initiatives undertaken in different jurisdictions worldwide. Indeed, most countries have established (or are on the verge of introducing) specific frameworks for OB, allowing the sharing of banking account data via standardised and secure interfaces (APIs) at the request of clients (Babina et al., 2024; OECD, 2024; OECD, 2023a).[1]Further, some countries have already considered extending these rules to financial services, thereby embracing Open Finance (OF) (OECD, 2023b).

Despite the growing interest in OB, it has been noted a lack of consensus on its definition (Briones de Araluze & Cassinello Plaza, 2022). Based on existing literature, four main connotations have been identified: the platformisation of the retail banking industry business model, a manifestation of the overall data-sharing trend applied to banking data, the interaction between the emergent ecosystem based on technological innovation (FinTech) and incumbent financial institutions, and the regulatory framework that, in some jurisdictions, bolsters the OB phenomenon (Briones de Araluze & Cassinello Plaza, 2022).

Nonetheless, as part of the broader framework of data policy initiatives aimed at empowering consumers with more control over their personal data, the unique features of OB have been investigated from many angles.

In particular, it has been noted that OB guarantees enhanced data privacy and security by replacing screen scraping as the most common method of accessing consumer data (Australian Government, 2023; US Consumer Financial Protection Bureau, 2023).[2]Additionally, by fostering consumer engagement and empowerment,

1. APIs are technology-driven protocols that allow computer systems or data sources to interact with other software, enabling applications to share data and functionality.
2. Screen scraping involves consumers sharing their login credentials with a third party, which then uses those credentials to access the consumer's account and retrieve data. This process can be used for both read and write access. With read access, the third party can view and collect data for their services, while with write access, they can also perform actions on the consumer's behalf. Due to these characteristics, screen scraping is seen as a risky data collection method that contradicts best practice cybersecurity guidelines. It exposes consumers to potential harm by offering little control over what data is collected or how it is used and shared, increasing the likelihood of inaccuracies,

OB can lead to more competitive markets (Borgogno & Colangelo, 2020a). In this regard, the idea of introducing interoperability through the so-called *in situ* data right (which allows users to use their data in its original location rather than moving it from the platform) has been seen as more effective from a competition policy perspective compared to simple data portability solutions (Martens, Parker, Petropoulos, & van Alstyne, 2021; Zetzsche, Arner, Buckley, & Weber, 2020).[3] It has been, therefore, suggested that OB may represent best practices and a blueprint to promote effective and workable interoperability beyond banking and financial industries, particularly in digital markets and Internet of Things (IoT) ecosystems (Borgogno & Colangelo, 2024). Moreover, insights from the UK experience have highlighted the importance of addressing the issue of the standardisation and technical definition of APIs (Dinçkol, Ozcan, & Zachariadis, 2023).

Overall, OB is expected to stimulate innovation, competition, and financial inclusion. Indeed, by putting customers in control of their data, OB provides opportunities to benefit from new, cheaper, and tailored services through FinTech (Babina et al., 2024). This would support more informed decisions, lower fees and switching costs, and ensure privacy and security.

Besides these benefits, potential risks have also been highlighted, suggesting that relevant trade-offs should be addressed when designing an OB framework. Indeed, each advantage coming from OB data-sharing rules goes hand in hand with a potential drawback. Notably, by empowering consumers to exploit their own data and thereby play an active role, OB also raises protection concerns, especially due to the lack of an adequate level of digital and financial literacy (Erel & Liebersohn, 2022; Wang Tok & Heng, 2022). This deficiency may expose vulnerable consumers to risks of manipulation and privacy and security harms. Similarly, on the competition policy side, data-sharing obligations imposed on banks also benefit non-financially regulated players, such as large online platforms (BigTechs) and data aggregators.[4] However, their entry may negatively affect competitive dynamics, financial

fraud, and data breaches.

3. Interoperability can be defined as the ability of two or more products or services to work together despite differences in interface, execution, or coding language. Conversely, data portability is the ability to port from data holder A to data holder B a bulk of data created during the use of a service by an individual. Therefore, data portability differs from data interoperability because it comes with a one-off transfer at a specified point in time.

4. Data aggregators, also known as API aggregators or API hubs, have emerged to address the proliferation of bank APIs. They act as intermediaries between banks and third-party operators, offering a standardised API that provides a single implementation point, allowing third parties to easily connect with various APIs without dealing with the complexities of data configuration and interface formatting.

stability, and monetary policy (Awrey & Macey, 2023; Croxson, Frost, Gambacorta, & Valletti, 2023; OECD, 2023c; de la Mano & Padilla, 2018).

Therefore, while OB policy goals are interconnected and can sometimes be mutually reinforcing, they may also involve significant trade-offs. Specifically, although empowering consumers by giving them control over their personal data can help achieve broader economic goals —such as fostering more competitive and innovative markets— the focus on competition and consumer empowerment may have unintended consequences for consumer protection, particularly in areas like privacy, security, and digital and financial literacy.

In this regard, concerns have been raised about the ability of OB to effectively protect users' personal data (Wolters & Jacobs, 2019). While fostering innovation and competition, the platformisation of banking and financial services can enable targeted individual marketing, exploitation of consumers' behavioral biases, misselling of financial services, and financial discrimination (OECD, 2022). Due to these negative externalities, some argue that the narrative of consumer technological empowerment overlooks the fact that technologies are often driven by industry interests and trends, rather than by a balanced assessment of their benefits and risks, and that the assumption that a liberalised market will provide better choices is flawed, as platformisation carries risks of monopolisation and market power abuses (Ferrari, 2022). Further, interpretative doubts and legal uncertainties arise concerning the interplay between OB regimes and data protection regulations. For instance, with respect to the EU landscape, several legal coordination issues have been identified, such as differing legal definitions of consent, ambiguity regarding their applicability to account data processing, the appropriate legal basis for account access and data processing, the sensitive nature of information in payment accounts, and the impracticality of separating it from other payment data (Ferretti, 2022).

Considering these trade-offs and the problems that need to be tackled for effective implementation, OB is not a single phenomenon but rather a highly differentiated one, with many shades depending on the country involved. Indeed, OB initiatives differ significantly, for instance, in terms of the type of regime (regulatory-driven v. market-led regime), the mandatory or voluntary nature of data sharing, eligibility rules and requirements for third parties seeking data access, the standardisation of APIs, and the provision of compensation for data access.

Rather than illustrating these differences, this paper aims to assess the consistency of OB policies. To this end, our analysis takes a novel perspective by investigating

the primary rationales that have inspired OB regulatory initiatives in some major countries (i.e., the EU, the UK, Australia, the US, India, Singapore). The premise is that, if OB is motivated by different justifications or market failures, it is unsurprising that one size does not fit all, and some countries have embraced their own versions of OB. Defining these primary rationales is essential for evaluating whether the specific features of OB solutions implemented in a country are consistent with the intended policy goals. Furthermore, such a comparative analysis would assist policymakers in countries considering the introduction of OB in properly designing an OB model that best fits their needs.

The paper is structured as follows. Section 1 analyses the main drivers of OB, providing a classification of major countries based on the justifications that have inspired their initiatives. Section 2 illustrates the different regulatory models and standardisation approaches adopted. Section 3 assesses OB policies by comparing their primary rationales with the models and technological solutions implemented. The conclusions summarise the main findings and policy recommendations.

1. Primary rationales for OB in various jurisdictions

OB can pursue several policy goals, such as increasing competition and innovation in the market, empowering consumers with control over their financial data, promoting open and secure data-sharing practices, and fostering financial inclusion. These policy objectives are typical in all OB initiatives. However, while a particular objective might clearly motivate an initiative, others may arise as consequential outcomes of pursuing different priorities. For example, while financial inclusion could serve as the main impetus behind an OB policy, it could also result from efforts to foster greater market competition, innovation, and digitalisation (Morris, 2024; Bianco & Vangelisti, 2022).

Further, it is essential to consider that the OB regime in each jurisdiction is implemented within the context of the financial ecosystem, including factors such as the concentration of market power in the hands of major players (typically incumbents or legacy banks), the incentives for market players to share data, and the financial access and literacy of consumers. Therefore, although the intended goals of OB are similar, the regulatory and institutional approaches differ in each jurisdiction.

This Section elaborates on the main obstacle each jurisdiction faces in implementing the OB regime effectively. Policymakers focus on a primary rationale they aim to achieve through regulation, which determines their approach to implementing OB. These primary rationales can be divided into three categories: (a) promoting

competition through technological innovation, (b) entrusting consumers with data rights as a key element of broader data policy initiatives, and (c) increasing financial inclusion.

(a) Competition: the EU and the UK

The EU was one of the first jurisdictions to make OB mandatory and, from the very beginning, it has been essentially guided by a competition policy goal. Indeed, as early as 2007, the first Payment Services Directive (PSD) aimed at enhancing competition in the retail payment market by harmonising payment transactions across the EU single market (Directive 2007/64/EC, 2007).

The emergence of new players due to the technical innovation driven by the FinTech evolution, along with the identified limitations of PSD in terms of legal certainty, security, and consumer protection, prompted EU institutions to revisit the Directive and establish a new, harmonised regulatory framework (Directive 2015/2366, 2015). In this context, the second Payment Services Directive (PSD2) introduced an access-to-account rule, mandating banks to provide access to customer account data to all authorised third payment service providers and to execute payment orders (Borgogno & Colangelo, 2020b; Polasik, Huterska, Iftikhar, & Mikula, 2020). This provision paved the way towards OB. Under PSD2, the European Central Bank and the European Banking Authority (EBA) are responsible for guaranteeing fair competition in the market.

The pro-competitive rationale is even more apparent in the UK, where the OB regime, based on the PSD2, has been operationalised by the antitrust authority, i.e. the Competition Markets Authority (CMA) (UK Competition and Markets Authority, 2017). Notably, OB in the UK was imposed as a remedy to address the adverse effects on competition in the retail and business banking sector, mainly to unbundle the services offered, remove incumbency advantages, and overcome consumer inertia (UK Competition and Markets Authority, 2016).

Therefore, the UK regime differs from the EU approach primarily in its technical implementation (Dinçkol, Ozcan, & Zachariadis, 2023). Indeed, while PSD2 is technology-agnostic, the UK promoted a standardised model of OB, requiring the largest nine banks to adopt common and open API standards, data formats, and security protocols provided by the OB Implementation Entity (OBIE) after consultations with the banks. This ensured an industry-wide standard, making it easier for other players to enter the market and for consumers to switch between different providers for various services.

(B) Data policy: Australia, Singapore, and the US

In other jurisdictions, OB emerged as part of data policies, resulting from broader governmental initiatives to create data-sharing frameworks. In this context, while some initiatives primarily focus on fostering consumer empowerment, others are justified on the grounds of ensuring security or promoting financial inclusion.

As previously mentioned, when examining the main rationales behind OB interventions, we do not wish to overlook their complementarity or their mutually reinforcing nature (Didenko, Jevglevskaja, & Buckley, 2024, pp. 12-16). However, trade-offs may sometimes arise between certain goals (e.g., competition and privacy; competition and financial inclusion). And even when these goals are closely interconnected, the primary justification advanced by policymakers to support a regulatory initiative may be crucial in evaluating the coherence of the means adopted to achieve it. This is particularly relevant in the case of competition and consumer empowerment. Indeed, empowering consumers with control over their data is expected to foster competition among different providers. Simultaneously, prioritising competition as a goal would provide consumers with more choices, thereby increasing their power.

However, regulation is not the primary tool to promote competition, but it may serve as a necessary means to facilitate data sharing, ensure certain standards of security, and foster digitalisation and financial inclusion. In terms of competition, regulatory intervention is instead justified only in cases of market failure, where it has been demonstrated that free and unrestricted competition is incapable of efficiently allocating resources, and the enforcement of traditional competition rules is likely to fail. This is precisely the scenario illustrated by policymakers in the EU and the UK.

In contrast, in Australia, the primary rationale for OB appears to be giving consumers the right to decide whether the data businesses hold about them should be shared with other providers.[5] Although the Australian government's interest, following the example of the UK, initially focused on a review of the banking industry (2017), the scope of its final intervention has expanded beyond that specific sector (Buckley, Jevglevskaja, & Farrell, 2022). Indeed, it is intended to encompass other sectors, regardless of the existence of a market failure. This approach stems from

5. For a different view, see Farrell (2023, pp. 30 and 36-38), acknowledging the different legal foundations of OB in Australia and the UK, but arguing that OB in both Australia and the UK has a strong focus on competition, whilst the UK had an initial stronger focus on consumer protection because of the influence of PSD2; and Didenko, Jevglevskaja, & Buckley (2024, p. 28), arguing that the promotion of competition plays a dominant role in the Australian initiative.

the Australian Government Productivity Commission's inquiry (2017) into the benefits and costs of options for improving availability and use of data which recommended the creation of a new economy-wide comprehensive data right.

Notably, drawing on the UK experience, the Australian Competition and Consumer Commission (ACCC) required the four major banks to share product reference data with accredited data recipients and mandated the adoption of a single set of API standards. However, from the outset, concerns regarding Australia's banking sector extended beyond the market power of the banks to include issues such as poor financial advice, the maladministration of life insurance claims, and market manipulation (Australian Parliament, 2016, p. 2). The initial report on OB emphasised that data sharing was introduced specifically to empower consumers by enhancing price transparency (Australian Parliament, 2016, p. 39). Similarly, the final report underscored the importance of giving consumers greater control over their information, resulting in increased choice and convenience (Australian Parliament, 2017). Accordingly, within the broader framework for reviewing the banking sector, the OB policy was explicitly designed to be "customer-focused" and to "be seen from the customer's perspective" (Australian Parliament, 2017, p. 5).

Therefore, despite adopting the UK model, the Australian policy maker aims to introduce an economy-wide data-sharing framework, known as the Consumer Data Right (CDR), which empowers consumers to share their data with any service provider they choose. The CDR focuses on OB as an information-gathering service, with the banking sector serving as the testing ground of this new framework, which is applicable across different sectors, including energy and telecommunications (Leach & McKay, 2022).[6]

As of now, the implementation of the CDR in the banking sector is complete, covering nearly 100% of the sector by household deposits. The roll-out in the energy sector began in 2022, with product data sharing starting on 1 October 2022, and consumer data sharing following on 15 November 2022 for initial energy retailers. However, the expansion into the telecommunications sector has been paused. Notably, in November 2021, the Australian Government (2021) released Treasury's final sectoral assessment report, which recommended that telecommunications be the third sector designated for the CDR. Nonetheless, in the 2023–24 budget, the Government committed to prioritising OF with non-bank lending (Australian Gov-

6. Under the CDR, the ACCC is responsible for enforcement, compliance, and management of the register, the Data Standards Body (DSB) develops technical standards, and the Office of the Australian Information Commissioner (OAIC) oversees privacy and confidentiality (see Didenko, Jevglevskaja, & Buckley, 2024, pp. 103-106).

ernment, 2023a), while pausing the CDR's implementation in the telecommunications sector (as well as in superannuation and insurance sectors) to allow time for the framework to mature in the initial sectors targeted. A strategic assessment is planned for the end of 2024 to guide future expansions and the implementation of action initiation (Australian Government, 2023b). An independent review commissioned by the Department of the Treasury revealed that the compliance costs associated with the CDR framework have significantly exceeded the original regulatory estimates, raising concerns about the continued pace of change (Richards, 2023). Consequently, the government announced a reset of the CDR and launched a new consultation on how to improve the CDR (Jones, 2024).

In a similar vein, the primary rationale behind OB in Singapore was to provide consumers with the ability to aggregate their financial information from different financial institutions in one place. OB has been enacted through the data portability obligation under the Personal Data Protection Act. However, Singapore's regime differs from those in the other jurisdictions examined, as it is a market-led collaborative approach promoted by the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) by publishing a non-binding API playbook to encourage banks to participate (Association of Banks in Singapore and Monetary Authority of Singapore, 2016; see also Remolina, 2019). Notably, the MAS, in collaboration with the financial institutions, developed an open public infrastructure known as the Singapore Financial Data Exchange (SGFinDex).[7] This gave consumers a consolidated view of their financial information for better financial planning. Therefore, in Singapore, OB essentially aimed to strengthen the digitalisation of the sector (Leong & Gardner, 2021).

Both Australia and Singapore have adopted a whitelist approach to OB, detailing implementation specifics related to data protection (Yeong & Hardoon, 2022). Despite similar goals and implementation, a key distinction exists between the two frameworks: Australia's OB is rights-based, while Singapore's is duty-based (Leong, 2020). Although data protection and consumer empowerment are related goals, Singapore's OB was developed primarily as a data policy focused on protecting consumer information by restricting banks from using consumer data without consent. In contrast, in Australia, data-sharing was enacted as a consumer right with safeguards embedded in the data protection regime. This difference may stem from the fact that, in Singapore, banks voluntarily began sharing data with fintech companies to improve consumer services. As a result, protecting data became a

7. Singapore Financial Data Exchange (SGFinDex): https://www.mas.gov.sg/development/fintech/sgfindex.

stronger priority than fostering competition and innovation. Consequently, Singapore's competition authority plays no role in implementing OB mandates.

Finally, after representing the main country embracing a market-led approach to OB, the US has switched to a regulatory-driven regime by mandating the sharing of financial data (Colangelo, 2024). In particular, activating the dormant Section 1033 of the Dodd-Frank Act enacted by the US Congress in 2010, the Consumer Financial Protection Bureau (CFPB) has recently adopted a rulemaking on "Personal Financial Data Rights" to facilitate the portability of consumer banking and financial data (US Consumer Financial Protection Bureau, 2024). The new rules require data providers to establish and maintain a developer interface for third parties to access consumer-authorised data under certain prescriptive performance and security specifications. Further, rather than dictating technical standards, the regulation supports industry standards appropriately developed within a data access framework. Finally, unlike most of the OB regimes, the US rule does not require data providers to initiate payments.

The policy priority inspiring the regulatory initiative is to protect consumers against fraudulent activities, rather than to foster market contestability. Indeed, with regard to market features, the US differs significantly from the EU and the UK, being the world's largest, most fragmented, and most diverse financial services industry (Awrey & Macey, 2023). The CFPB explicitly acknowledges this, noting that any differences between its approach and those of other jurisdictions are appropriate given "the particular market and regulatory frameworks applicable to the U.S." (US Consumer Financial Protection Bureau, 2024, pp. 57-58). Notably, "American consumers already expect third party data access capabilities, and the US market consists of a higher number of depository institutions (and card issuers) than most other jurisdictions." (US Consumer Financial Protection Bureau, 2024, p. 181).

Against this backdrop, the CFPB's intervention aims to promote data sharing by ensuring trust and security for consumers, moving the market away from risky data collection practices. Accordingly, the main justification for this top-down intervention is to outlaw screen scraping, which is considered problematic for data privacy, security, and accuracy (Chopra, 2022). From a comparative perspective, it is noteworthy that the recent evaluation report on the European regime highlights its success in protecting user data and enhancing the security of remote payments through the introduction of strong customer authentication (SCA). This system requires two authentication factors, which can be based on knowledge (e.g., a password), possession (e.g., a card), or inherence (e.g., a fingerprint) (European Commission, 2023a). For example, an analysis of the Italian market, using data reported by

payment service providers to the Bank of Italy, estimates that SCA reduces the risk of fraud by 60 percent for card-based remote payments and by 80 percent for e-money transactions (Cologgi, 2023).

(C) Financial inclusion: India

In an emerging economy like India, where a significant part of the population does not have access to financial services, the OB's primary rationale is, instead, to increase financial inclusion (Carrière-Swallow, Haksar, & Patnam, 2021). As a result, the OB framework is a part of the government's initiative to build a digital public infrastructure (DPI), also known as the India stack (Alonso et al., 2023). Under this initiative, the first step in enhancing financial inclusion was to create a verifiable identity (known as Aadhaar), which was then used as a foundation for other financial infrastructure, the most influential being the interoperable payment infrastructure, known as the Unified Payments Interface (UPI). The stack comprises three layers of infrastructure: (i) the identity layer for digitalisation of documentation and verification, (ii) the payments layer UPI, and (iii) a data or consent layer (Desai, Manoharan, Shiva Jayanth, & Zack, 2024).

Like Singapore, India's OB system has been developed by the Central Bank, specifically the Reserve Bank of India (RBI). However, unlike Singapore, India did not have a data protection framework in place at the time OB was adopted. As a result, OB was developed under the Data Empowerment and Protection Architecture (DEPA), a joint public-private initiative aimed at improving data governance (NITI Aayog, 2020).

2. Regulatory and technical solutions

Against the overview of OB's primary rationales, this Section explores if and how these rationales have influenced policymakers' decisions regarding the implementation of the OB regime in their respective jurisdictions. Notably, the Section elaborates on the regulatory and technical solutions adopted and their alignment with the rationale and the financial ecosystem of the jurisdiction at issue. In this regard, the discussion focuses on various endorsed approaches concerning the nature of data-sharing obligations (voluntary vs. mandatory) and the standardisation process (top-down vs. market-led), which are summarised in Table 1.

From the very beginning, it is worth noting that the implementation of the Australian OB regime is similar to that of the UK. In both countries, OB is mandatory and the standards are set by a regulated body. However, the implications of the

different primary rationale are evident in the scope of implementation. For example, Australia's primary rationale was to create a data-sharing framework, so OB applies to more entities, unlike the UK's limited applicability to only banks. Additionally, in Australia, OB serves as the testing ground for fostering data sharing across several sectors. Accordingly, a reciprocal obligation to share data is also imposed on data recipients.

In Singapore, despite sharing the same policy goal as Australia, the approach to OB differs. This difference reflects the fact that the banking sector was already competitive due to existing regulatory policies and a highly developed infrastructure. Therefore, OB was not made mandatory as major players had already adopted it independently. For example, DBS Bank created the largest API developer platform (DBS Bank, 2017). Consequently, OB emerged as a market-led initiative. Nonetheless, although the participation is voluntary, the MAS fosters a conducive environment for a smooth transition to an open-architecture banking sector. This is achieved by publishing non-binding API standards and providing enabling infrastructure through SGFinDex, which ensures privacy by design with encrypted user financial data that SGFinDex cannot read or store. These mechanisms helped MAS bring together various players to build the necessary ecosystem (Kwan Chow & Fan Pei, 2019).

As OB has been introduced in the EU and the UK by the same legislative initiative (i.e., PSD2), they share both the competitive rationale and the mandatory nature of the data-sharing obligation. However, they differ significantly in their standardisation approaches. Indeed, as opposed to the top-down solution adopted in the UK, the EU has refrained from publicly mandating API standardisation, allowing banks to create their own data-sharing interfaces or participate in privately-led standardisation initiatives. This decision was based on the concern that a common API standard could hinder innovation and dynamic competition between standards.

Interestingly, the US is following the EU's approach regarding the nature of the data-sharing obligation and the standardisation process, despite the legislative initiative being inspired by a different rationale. Further, it has been noted that these similarities with EU solutions contrast with the unique features of the US market (Colangelo, 2024; Awrey & Macey, 2023). Notably, OB already exists in the US without a regulatory obligation. In addition, the US banking and financial sector is highly fragmented. Consequently, although institutions have undertaken initiatives to promote API standards (including private standard-setting bodies like the Financial Data Exchange), these efforts have been considered controversial and the market is characterised by a relatively concentrated share of data aggregators,

which raises different competitive concerns compared to those addressed in the EU (US Consumer Financial Protection Bureau, 2023).

In this scenario, India has adopted a unique combination of data-sharing obligations and standardisation solutions. Indeed, OB is facilitated through an account aggregator (AA) framework (Reserve Bank of India, 2016). AAs are data fiduciaries, registered and regulated by the RBI, acting as intermediaries between Financial Information Providers (FIPs), such as banks, insurance providers, tax platforms, and Financial Information Users (FIUs), which include entities regulated by financial sector regulators. AAs connect customers to multiple FIPs through standardised API interfaces developed by the Reserve Bank Information Technology Private Limited (ReBIT), a subsidiary of the RBI. The information transmitted from FIPs to AAs, and subsequently to FIUs, is encrypted. Further, to mitigate the risks of data misuse, AAs cannot use or access data for any other purpose.

Nonetheless, despite such a top-down standardisation approach, participation in the OB (i.e., the AA framework) is voluntary. This is because, unlike in other jurisdictions, India's banking sector was competitive even before the adoption of OB. As a result, much like in Singapore, India's competition authority plays no role in regulating OB policies. Moreover, data access is reciprocal, therefore, if an entity is a FIU, then it also needs to be registered as a FIP. This stands in stark contrast to most of the other experiences analysed in this paper, where data-sharing provisions are instead asymmetric. Despite the purported goal of ensuring a level informational playing field, fostering digitalisation, and promoting data sharing to empower consumers, other countries merely impose on banks the duty to grant access to third-party providers.

TABLE 1: Data sharing and standardisation approaches

JURISDICTION	YEAR OF ADOPTION	PRIMARY RATIONALE	REGULATORY AUTHORITY	DATA SHARING	STANDARDISATION
Australia	2020	Consumer empowerment	ACCC, OAIC	Mandatory and reciprocal	Top-down
EU	2015	Competition	Commission,EBA	Mandatory and asymmetric	Market-led
India	2021	Financial inclusion	RBI	Voluntary and reciprocal	Top-down
Singapore	2016	Consumer	MAS	Voluntary	Market-led

JURISDICTION	YEAR OF ADOPTION	PRIMARY RATIONALE	REGULATORY AUTHORITY	DATA SHARING	STANDARDISATION
		empowerment			
UK	2017	Competition	CMA, OBIE	Mandatory and asymmetric	Top-down
US	2024	Data privacy and security	CFPB	Mandatory and asymmetric	Market-led

3. Looking for consistency in OB regimes: matching rationales and models

By mapping primary rationales (*supra* Section 1) and models in terms of data-sharing obligations and standardisation solutions (*supra* Section 2), the comparative analysis reveals the many nuances of OB. While some countries adopt similar models despite different rationales (i.e., the EU and the US), others share the same rationale but employ different models in terms of a regulator-led or market-led approach (i.e., the EU vs. the UK, and Australia vs. Singapore). Additionally, some countries represent unique experiences, such as India.

Therefore, the variation in models and approaches among the examined jurisdictions does not necessarily reflect different policy goals pursued through the OB regime. Further, starting from each primary rationale supporting OB initiatives, it is still necessary to assess the consistency of OB policies by evaluating whether the regulatory and technical solutions endorsed fit with the intended rationale.

When the primary rationale is to increase competition in the market, it makes sense to have a mandatory obligation to share data, as seen in the EU and the UK. However, in both cases, the obligation is asymmetric as it is only imposed on banks. Such an approach is at odds with the policy goal as a reciprocal data-sharing obligation on data recipients would promote greater competition and enhance innovation by fostering the development of new products and services (Australian Government, 2017). A reciprocal obligation would also help to alleviate competition concerns by preventing disadvantages for banks mandated to share data with new players (e.g., FinTechs, BigTechs, and data aggregators), who might gain an advantageous position over time (Carr, Pujazon & Urbiola, 2018; de la Mano & Padilla, 2018).

In such a scenario, the UK's top-down standardisation approach has proven to be

more effective than the European market-led alternative. While the evaluation report revealed limits to PSD2's effectiveness in achieving a level playing field and mixed success in the uptake of OB in the EU (European Commission, 2023a), the UK celebrates the success of its model, citing significant take-up and accelerating growth (UK Joint Regulatory Oversight Committee, 2023; UK Government, 2022). Further support for the UK solution comes from the recent EU proposal to introduce Open Finance (European Commission, 2023b). Indeed, as the consultation indicated the lack of standardisation as a major obstacle to data sharing in finance (European Commission, 2023c), the proposal includes a requirement for market participants to jointly develop common standards for customer data and interfaces as part of financial data-sharing schemes.

If the primary goal is consumer empowerment, implementing a mandatory data-sharing obligation appears essential as well. However, the voluntary approach adopted in Singapore may be an acceptable exception, given the widespread adoption of OB in the country. Additionally, when considering the nature of this obligation, consumer empowerment does not necessarily require reciprocity. As previously mentioned, a reciprocal data-sharing obligation mainly serves to promote market competition. Rather, in this case, it seems appropriate to broaden the scope of the obligation with reference to both the entities and the data covered. Finally, regarding technical solutions, a top-down approach seems preferable. High standardisation would empower consumers by making it easier for them to exercise their data rights and receive offers from other providers.

A mandatory data-sharing obligation is unnecessary and should not be imposed when the primary rationale for the OB initiative is to ensure data privacy and security. Indeed, it is unclear how imposing a data-sharing obligation would address this issue. The same doubt applies to the nature (reciprocal or asymmetric) of such an obligation.

However, as discussed, data privacy and security may be negatively impacted by the externalities generated in the pursuit of competition goals, which are often prioritised particularly in countries with highly concentrated markets and persistent competitive challenges (such as the EU and UK, unlike the US). Similarly, an empirical study of the EU credit market found that an excessive focus on data policies may limit the long-term impact of OB on fostering greater competition and innovation (Lauridsen, 2024). In these scenarios, it is essential to strike a balance between promoting competition and ensuring a high level of security in data access and exchange. In this regard, the solution proposed by the European Commission (2023d) in its PSD2 reform appears compelling. It aims at prohibiting screen scrap-

ing by requiring the use of dedicated interfaces for OB purposes and eliminating the option for third-party providers to rely on fallback interfaces (see also Wolters & Jacobs, 2019).[8]As a result, access to consumer data would be restricted to a standardized interface and secured by a multi-factor authentication system, similar to one successfully implemented by the PSD2. In such a case, a top-down standardisation approach may help.

An outright ban on screen scraping, along with the availability of a standardised interface, would be especially crucial in markets with a significant presence of data aggregators. In this scenario, it might also be beneficial to look at the Indian OB regime, where data is encrypted, and account aggregators cannot access or use the data for any other purpose. This is again achieved through a top-down solution, i.e., an enabling infrastructure provided by the regulator and the requirement for each player to be licensed, ensuring compliance with data security and privacy safeguards.

Finally, if the policy goal pursued is to enhance financial inclusion, the promotion of OB involves relevant trade-offs. While technological innovation in banking and finance can promote financial inclusion and help consumers make informed choices, it also raises risks of discrimination, manipulation, and exploitation of vulnerable customers, particularly in areas with low levels of digital and financial literacy. Therefore, as highlighted in the literature, the policy goal of promoting innovative entry can sometimes come into conflict with the financial inclusion and the customers who benefit the most may be those who already have credit access (Babina et al., 2024; Croxson, Frost, Gambacorta & Valletti, 2023; Preziuso, Koefer & Ehrenhard, 2023; OECD, 2022; Wang Tok & Heng, 2022; Philippon, 2019). These limitations do not justify introducing a mandatory data-sharing obligation in an OB regime that aims to promote financial inclusion.

TABLE 2: Optimal regulatory and technical solutions according to different rationales

PRIMARY RATIONALE	DATA SHARING	STANDARDISATION
Competition	Mandatory and reciprocal	Top-down

8. This represents one the major critics to the US proposal since, despite the CFPB's concerns about credential-based data access and screen scraping, many participants to the public consultation complained that the new rules would allow third parties and data aggregators to continue screen scraping from a data provider even after an interface compliant with the proposal's requirements has been implemented. For an analysis, see Colangelo (2024). Conversely, see Australian Government (2023c) evaluating the possibility to introduce an outright ban on screen scraping in sectors where the regulated data access regime is a viable alternative.

PRIMARY RATIONALE	DATA SHARING	STANDARDISATION
Consumer empowerment	Mandatory	Top-down
Data privacy and security	Voluntary	Top-down
Financial inclusion	Voluntary	Top-down

Our findings, summarised in Table 2, should help both policymakers evaluating amendments to their current regime (e.g., European Commission, 2023d; European Commission, 2023e) and policymakers in countries considering the introduction of OB to design a model that best suits their needs. About the latter case, for instance, the Canadian Government Department of Finance has recently launched a consultation on 'Strengthening Competition in the Financial Sector' (Government of Canada, 2023) and the Competition Bureau urged policymakers to prioritise an OB regulatory design aimed at nurturing competition and innovation in the financial sector by challenging established providers and enabling new service providers (Canadian Competition Bureau, 2024).

Given the concerns on concentration and competition in Canada's banking sector reported by the Department of Finance and the Competition Bureau, the primary rationale of a prospective OB regime is clearly identified. According to our analysis, Canadian policymakers should therefore be inspired from the UK experience but should also introduce a relevant adjustment by imposing a reciprocal data-sharing obligation on all financial service providers involved. This is exactly what the Competition Bureau suggested to the Canadian Government. Specifically, the adoption of a common API standard with principles and oversight established in legislation, and the promotion of a reciprocal access to in-scope data among participants.

Concluding remarks

Despite its growing success and widespread adoption around the world, OB struggles to present a coherent identity. Each country has seemingly developed its own approach to OB, leading to various models based on different rationales, data-sharing obligations, and standardisation processes.

Against this backdrop, this paper has drawn insights from experiences in the EU, UK, Australia, the US, India, and Singapore to evaluate the consistency of OB policies. To achieve this, the paper first identified the primary rationales supporting OB initiatives in these countries and then examined their data-sharing and standardisation approaches. After all, if OB is driven by various justifications or market fail-

ures, it's not surprising that a single approach doesn't work for every jurisdiction.

Our comparative analysis served as the foundation for proposing regulatory and technical solutions that better align with the intended policy goals of an OB regime. The findings suggest significant revisions to current regimes and offer guidance to policymakers evaluating initiatives to promote OB. For instance, in Canada, where there is an ongoing discussion about OB regulatory design, our findings fully support the recommendations made by the Competition Bureau to the government.

References

Alonso, C., Bhojwani, T., Hanedar, E., Prijardini, D., Uña, G., & Zhabska, K. (2023). *Stacking up the benefits: Lessons from India's digital journey* (Working Paper No. 78). IMF. https://www.imf.org/en/Publications/WP/Issues/2023/03/31/Stacking-up-the-Benefits-Lessons-from-Indias-Digital-Journey-531692.

Association of Banks in Singapore and Monetary Authority of Singapore. (2016). *Financial world. Finance-as-a-service: API playbook*. https://abs.org.sg/docs/library/abs-api-playbook.pdf

Australian Government. (2017). *Review into open banking: Giving customers choice, convenience and confidence*. https://treasury.gov.au/consultation/c2018-t247313

Australian Government. (2021). *Consumer data right – telecommunications sectoral assessment – final report*. https://treasury.gov.au/publication/p2021-225262

Australian Government. (2023a). *Consumer data right rules – expansion to the non-bank lending sector*. https://treasury.gov.au/consultation/c2023-434434-expansion

Australian Government. (2023b). *Consumer data right rules – expansion to the telecommunications sector and other operational enhancements*. https://treasury.gov.au/consultation/c2022-315575

Australian Government. (2023c). *Screen scraping – policy and regulatory implications*. https://treasury.gov.au/consultation/c2023-436961.

Australian Government Productivity Commission. (2017). *Data availability and use. Productivity commission inquiry report* (No. 82). https://www.pc.gov.au/inquiries/completed/data-access/report

Awrey, D., & Macey, J. (2023). The promise & perils of open finance. *Yale Journal of Regulation*, *40*(1), 1–59.

Babina, T., Bahaj, S., Buchak, G., De Marco, F., Foulis, A., Gornall, W., Mazzola, F., & Yu, T. (2024). *Customer data access and Fintech entry: Early evidence from open banking* (Working Paper No. 32089; p. w32089). National Bureau of Economic Research. https://doi.org/10.3386/w32089

Basel Committee on Banking Supervision. (2019). *Report on open banking and application programming interfaces*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d486.htm

Bianco, M., & Vangelisti, M. I. (2022). Open banking and financial inclusion. *European Economy*, *1*,

81–97.

Borgogno, O., & Colangelo, G. (2020a). Consumer inertia and competition-sensitive data governance: The case of open banking. *Journal of European Consumer and Market Law*, *9*(4), 143–150.

Borgogno, O., & Colangelo, G. (2020b). Data, innovation and competition in finance: The case of the access to account rule. *European Business Law Review*, *31*(Issue 4), 573–610. https://doi.org/10.54648/EULR2020023

Briones de Araluze, G. K., & Cassinello Plaza, N. (2022). Open banking: A bibliometric analysis-driven definition. *PLOS ONE*, *17*(10), e0275496. https://doi.org/10.1371/journal.pone.0275496

Buckley, R. P., Jevglevskaja, N., & Farrell, S. (2022). Australia's data-sharing regime: Six lessons for Europe. *King's Law Journal*, *33*(1), 61–91. https://doi.org/10.1080/09615768.2022.2034582

Buckley, R. P., Zetzsche, D., Arner, D. W., & Weber, R. H. (2020). The evolution and future of data-driven finance in the EU. *Common Market Law Review*, *57*(Issue 2), 331–360. https://doi.org/10.54648/COLA2020030

Canadian Competition Bureau. (2024). *Strengthening competition in the financial sector: Submission by the competition bureau*. https://competition-bureau.canada.ca/how-we-foster-competition/promotion-and-advocacy/strengthening-competition-financial-sector-submission-competition-bureau

Carr, B., Pujazon, D., & Urbiola, P. (2018). *Reciprocity in customer data sharing frameworks*. Institute of International Finance. https://www.iif.com/portals/0/Files/private/32370132_reciprocity_in_customer_data_sharing_frameworks_20170730.pdf

Carrière-Swallow, Y., Haksar, V., & Patnam, M. (2021). *India's approach to open banking: Some implications for financial inclusion* (Working Paper No. 52). IMF. https://www.imf.org/en/Publications/WP/Issues/2021/02/26/Indias-Approach-to-Open-Banking-Some-Implications-for-Financial-Inclusion-50049

Chopra, R. (2022). *Director Chopra's prepared remarks at money 20/20*. Consumer Financial Protection Bureau. https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/

Colangelo, G. (2024). Open banking goes to Washington: Lessons from the EU on regulatory-driven data sharing regimes. *Computer Law & Security Review*, *54*, 106018. https://doi.org/10.1016/j.clsr.2024.106018

Colangelo, G., & Borgogno, O. (2024). Shaping interoperability for the internet of things: The case for ecosystem-tailored standardisation. *European Journal of Risk Regulation*, *15*(1), 137–152. https://doi.org/10.1017/err.2023.8

Cologgi, M. (2023). The impact of regulation on retail payments security: Evidence from Italian supervisory data. *Finance Research Letters*, *54*, 103799. https://doi.org/10.1016/j.frl.2023.103799

Croxson, K., Frost, J., Gambacorta, L., & Valletti, T. (2023). Platform-based business models and financial inclusion: Policy trade-offs and approaches. *Journal of Competition Law & Economics*, *19*(1), 75–102. https://doi.org/10.1093/joclec/nhac010

DBS Bank. (2017). *Reimagining banking, DBS launches world's largest banking API developer platform*. https://www.dbs.com/newsroom/Reimagining_banking_DBS_launches_worlds_largest_banking_API_developer_platform

De La Mano, M., & Padilla, J. (2018). Big tech banking. *Journal of Competition Law & Economics*, *14*(4),

494–526. https://doi.org/10.1093/joclec/nhz003

Desai, A., Manoharan, A. P., Jayanth, S. S., & Zack, S. (2024). Public value creation through combined consumption of multiple public services – case of India Stack. *International Journal of Public Administration*, *47*(9), 600–611. https://doi.org/10.1080/01900692.2023.2243401

Didenko, A., Jevglevskaja, N., & Buckley, R. P. (2024). *Customer data sharing frameworks. Twelve lessons for the world*. Routledge.

Dinçkol, D., Ozcan, P., & Zachariadis, M. (2023). Regulatory standards and consequences for industry architecture: The case of UK open banking. *Research Policy*, *52*(6), 104760. https://doi.org/10.1016/j.respol.2023.104760

Directive 2007/64/EC. (2007). *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance)*. European Parliament and Council. https://eur-lex.europa.eu/eli/dir/2007/64/oj/eng

Directive (EU) 2015/2366. (2015). *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)*. European Parliament and Council. http://data.europa.eu/eli/dir/2015/2366/oj

Erel, I., & Liebersohn, J. (2022). Can fintech reduce disparities in access to finance? Evidence from the Paycheck Protection Program. *Journal of Financial Economics*, *146*(1), 90–118. https://doi.org/10.1016/j.jfineco.2022.05.004

European Commission. (2023a). *Commission staff working document impact assessment report accompanying the document proposal for a Regulation of the European Parliament and of the Council on a framework for financial data access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554* (Working Document No. 52023SC0224). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023SC0224

European Commission. (2023b). *Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the internal market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0366

European Commission. (2023c). *Proposal for a Regulation of the European Parliament and of the Council on a framework for financial data access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0360

European Commission. (2023d). *Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0367

European Commission. (2023e). *Report on the review of Directive 2015/2366/EU of the European Parliament and of the Council on payment services in the internal market*.

Farrell, S. (2023). *Banking on data: Evaluating open banking and data rights in banking law*. Wolters Kluwer.

Ferrari, V. (2022). The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda. *Computer Law & Security Review*, *45*, 105687. https://doi.org/10.1016/j.clsr.2

022.105687

Ferretti, F. (2022). Open banking: Gordian legal knots in the uncomfortable cohabitation between the PSD2 and the GDPR. *European Review of Private Law*, *30*(Issue 1), 73–102. https://doi.org/10.54648/ERPL2022004

Government of Canada. (2023). *Consultation on strengthening competition in the financial sector*. https://www.canada.ca/en/department-finance/programs/consultations/2023/consultation-on-strengthening-competition-in-the-financial-sector.html

Jones, S. (2024). *Albanese government to reset consumer data right*. https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/albanese-government-reset-consumer-data-right

Kwan Chow, H., & Fan Pei, S. (2018). Financial sector in Singapore. In U. Volz, P. J. Morgan, & N. Yoshino (Eds.), *Routledge handbook of banking and finance in Asia* (1st ed., pp. 165–179). Routledge. https://doi.org/10.4324/9781315543222

Lauridsen, N. (2024). *Does regulatory-driven innovation affect traditional financial intermediaries? Evidence from open banking frameworks* (Working Paper No. 2024/11). EUI Robert Schuman Centre for Advanced Studies. https://cadmus.eui.eu/bitstream/handle/1814/76794/RSC_WP_2024_11.pdf?sequence=1&isAllowed=y

Leach, J., & McKay, J. (2022). The Australian consumer data right: The promise of open data. In L. Jeng (Ed.), *Open banking* (1st ed., pp. 201–234). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197582879.003.0011

Leong, E. (2020). Open banking: The changing nature of regulating banking data – a case study of Australia and Singapore. *Banking & Finance Law Review*, *35*(3), 443–469.

Leong, E., & Gardner, J. (2021). Open banking in the UK and Singapore: Open possibilities for enhancing financial inclusion. *Journal of Business Law*, *5*, 424–453.

Martens, B., Parker, G., Petropoulos, G., & Alstyne, M. (2021). *Towards efficient information sharing in network markets (Working Paper 12* [Working Paper]. Bruegel. https://www.bruegel.org/2021/11/towards-efficient-information-sharing-in-network-markets/

Morris, J. (2024). *Digital payments and financial inclusion* [Issue Brief]. ICLE. https://laweconcenter.org/resources/digital-payments-and-financial-inclusion/

NITI Aayog. (2020). *Data empowerment and protection architecture. A secure consent-based data sharing framework to accelerate financial inclusion [Draft for discussion]*. https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf

OECD. (2023a). *Data portability in open banking: Privacy and other cross-cutting issues* (Policy Paper No. 348; OECD Digital Economy Papers, Vol. 348). https://doi.org/10.1787/6c872949-en

OECD. (2023b). *Open finance policy considerations* (Policy Paper No. 36; OECD Business and Finance Policy Papers, Vol. 36). https://doi.org/10.1787/19ef3608-en

OECD. (2023c). *Shifting from open banking to open finance: Results from the 2022 OECD survey on data sharing frameworks* (Policy Paper No. 24; OECD Business and Finance Policy Papers, Vol. 24). https://doi.org/10.1787/9f881c0c-en

OECD. (2024). *Competition, fintechs and open banking: An overview of recent developments in Latin America and the Caribbean* (Policy Paper No. 313; OECD Roundtables on Competition Policy Papers,

Vol. 313). https://doi.org/10.1787/de9fe6b4-en

OECD/European Commission. (2022). *Policy brief on access to finance for inclusive and social entrepreneurship: What role can fintech and financial literacy play?* (Working Paper No. 2022/06; OECD Local Economic and Employment Development (LEED) Papers, Vol. 2022/06). https://doi.org/10.1787/77a15208-en

Parliament of the Commonwealth of Autralia. (2016). *Review of the four major banks* (No. 1). https://www.aph.gov.au/parliamentary_business/committees/house/economics/four_major_banks_review/report

Philippon, T. (2019). *On fintech and financial inclusion* (Working Paper No. 26330; p. w26330). National Bureau of Economic Research. https://doi.org/10.3386/w26330

Polasik, M., Huterska, A., Iftikhar, R., & Mikula, Š. (2020). The impact of payment services directive 2 on the paytech sector development in Europe. *Journal of Economic Behavior & Organization*, *178*, 385–401. https://doi.org/10.1016/j.jebo.2020.07.010

Preziuso, M., Koefer, F., & Ehrenhard, M. (2023). Open banking and inclusive finance in the European Union: Perspectives from the Dutch stakeholder ecosystem. *Financial Innovation*, *9*(1), 111. https://doi.org/10.1186/s40854-023-00522-1

Remolina, N. (2019). Open banking: Regulatory challenges for a new form of financial intermediation in a data-driven world. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3475019

Reserve Bank of India. (2016). *Master direction—Non-banking financial company—Account aggregator (reserve bank) directions*. https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598.

Richards, H. (2023). *Consumer data right compliance costs review*. Treasury of the Australian Government. https://treasury.gov.au/publication/p2024-512569

Rulemaking on Personal Financial Data Rights, Pub. L. No. 2024–25079 (2024). https://files.consumerfinance.gov/f/documents/cfpb_personal-financial-data-rights-final-rule-reg-text_2024-10.pdf

The Retail Banking Market Investigation Order 2017 (2017). https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017

UK Competition and Markets Authority. (2016). *Retail banking market investigation (Final report)*. https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk#final-report

UK Government. (2022). *Joint statement by HM Treasury, the CMA, the FCA and the PSR on the future of open banking* [Policy Paper]. https://www.gov.uk/government/publications/joint-statement-by-hm-treasury-the-cma-the-fca-and-the-psr-on-the-future-of-open-banking

UK Joint Regulatory Oversight Committee. (2023). *Recommendations for the next phase of open banking in the UK*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf

Wang Tok, Y., & Heng, D. (2022). *Fintech: Financial inclusion or exclusion?* (Working Paper No. 80). IMF. https://www.imf.org/en/Publications/WP/Issues/2022/05/06/Fintech-Financial-Inclusion-or-Exclusion-517619

Wolters, P. T. J., & Jacobs, B. P. F. (2019). The security of access to accounts under the PSD2. *Computer Law & Security Review*, *35*(1), 29–41. https://doi.org/10.1016/j.clsr.2018.10.005

Yeong, Z. K., & Hardoon, D. R. (2022). Taking your data with you: Singapore's approach to data portability. In L. Jeng (Ed.), *Open Banking* (1st ed., pp. 107–126). Oxford University PressNew York. ht tps://doi.org/10.1093/oso/9780197582879.003.0007

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with

UNIVERSITY OF TARTU
Johan Skytte Institute of
Political Studies