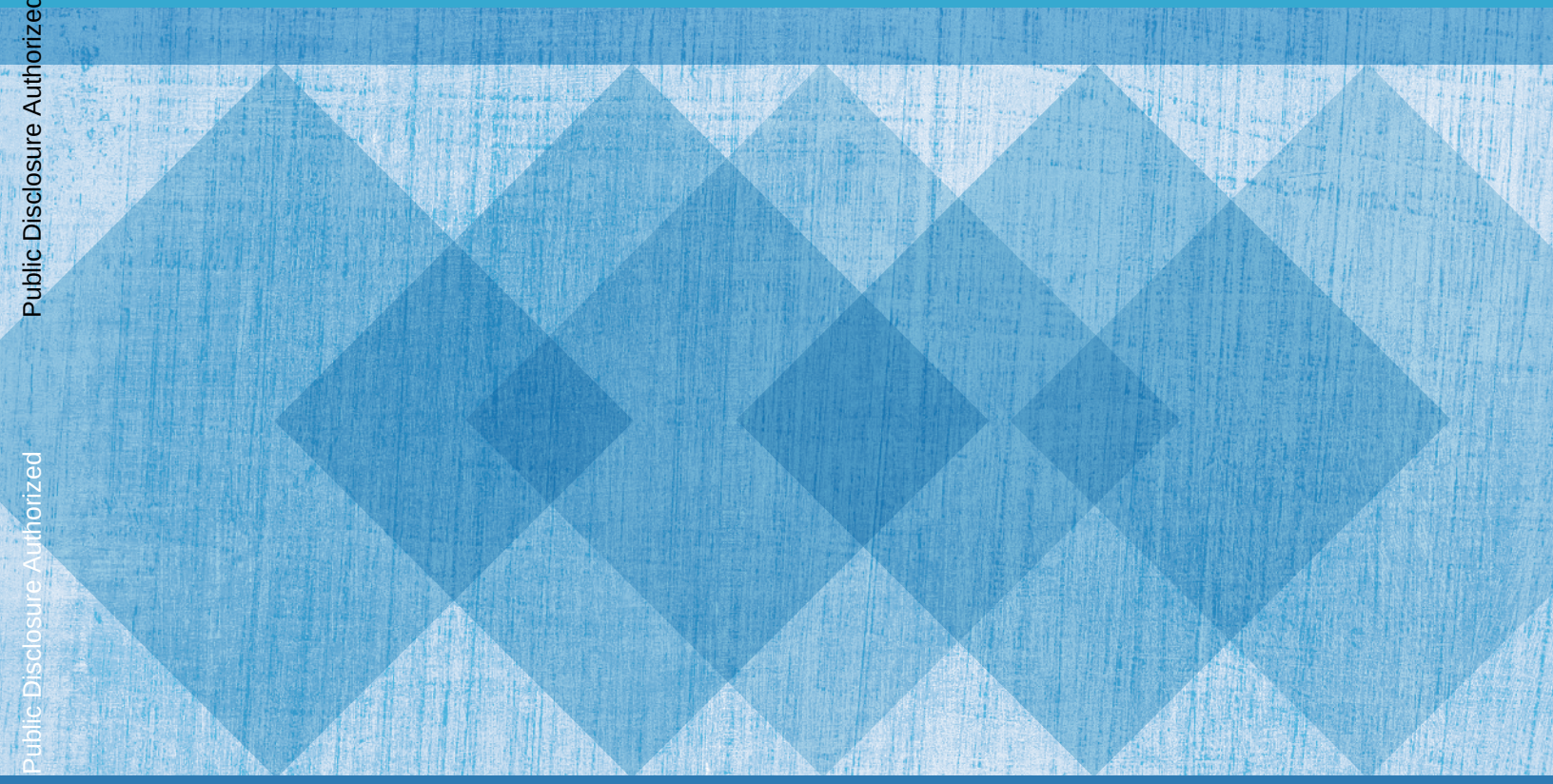
TECHNICAL NOTE

The Role of Consumer Consent in Open Banking

FINANCIAL INCLUSION SUPPORT FRAMEWORK

DECEMBER 2021



WORLD BANK GROUP

Ministry of Foreign Affairs of the Netherlands

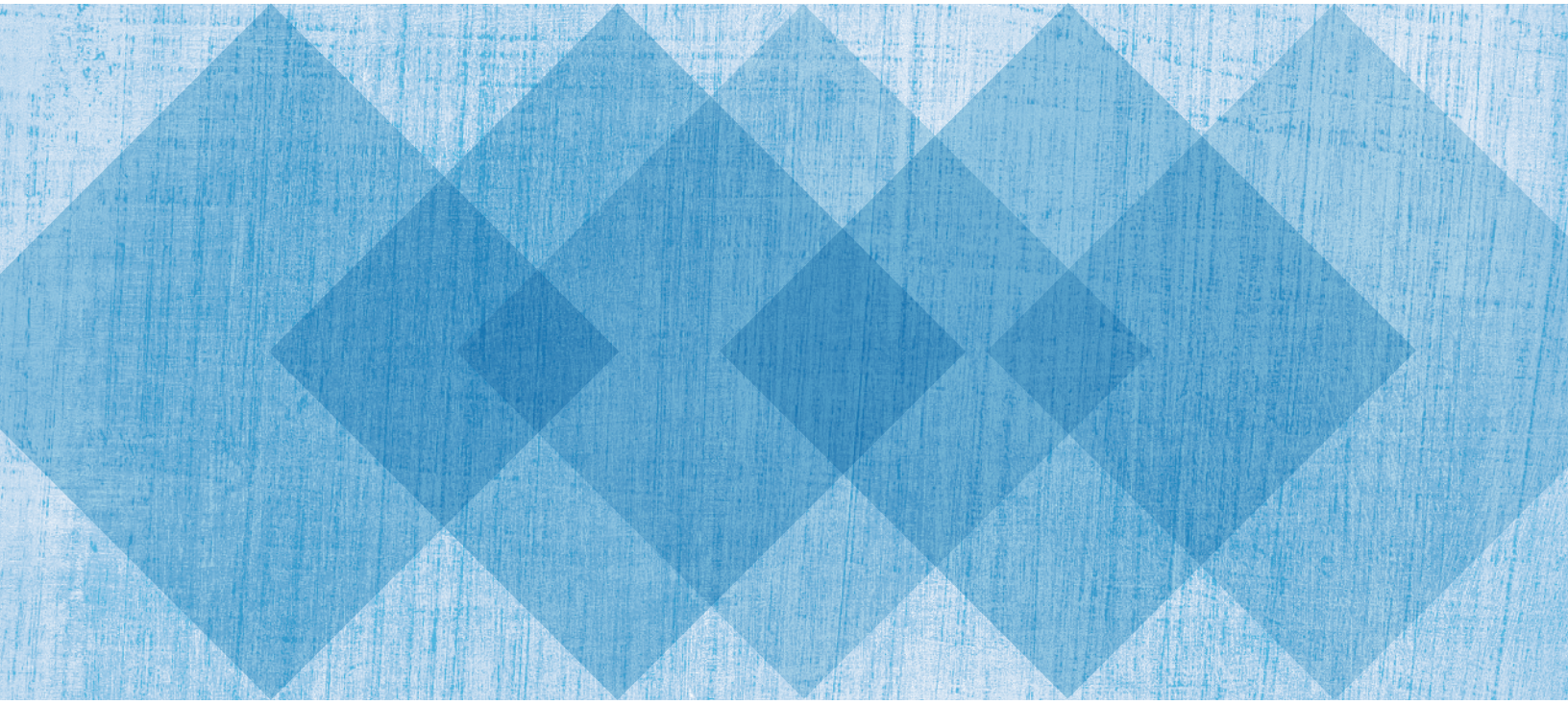
FINANCE, COMPETITIVENESS &
INNOVATION GLOBAL PRACTICE

TECHNICAL NOTE

The Role of Consumer Consent in Open Banking

FINANCIAL INCLUSION SUPPORT FRAMEWORK

DECEMBER 2021



WORLD BANK GROUP

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

CONTENTS

BOXES

FIGURES

TABLES

ACKNOWLEDGMENTS

This report was coauthored by Clare Sullivan, Managing Director of Cyber SMART, Georgetown University; Margaret Miller, Lead Financial Sector Economist, World Bank Group; and Fredesvinda Montes, Senior Financial Sector Specialist, World Bank Group. The report was funded through the Financial Inclusion Support Framework program funded by the Bill and Melinda Gates Foundation and is part of a series of documents on consumer risks in the context of digital financial services and fintech.

Peer reviewers and others who provided valuable guidance for this report included Graciela Miralles Murciego, Harish Natarajan, and James Neumann (World Bank); and Ariadne Plaitakis (Consultative Group to Assist the Poor).

All errors and omissions are the sole responsibility of the authors.

LIST OF ACRONYMS

ACCC	Australian Competition and Consumer Commission
AISP	account-information service provider
API	application programming interface
CCA	Competition and Consumer Act of 2010 (Cth)
CDR	Consumer Data Right
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
LGPD	General Personal Data Protection Law (*Lei Geral de Proteção de Dados Pessoais*)
OAIC	Office of the Australian Information Commissioner
PISP	payment-initiation service provider
PPD	Federal Law on the Protection of Personal Data Held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*)
PSD2	Revised Payment Systems Directive
TPP	third-party provider
WP29	Article 29 Working Party

EXECUTIVE SUMMARY

ABSTRACT: Open banking schemes provide consumers with more choice and new financial products and services through the use of technology, particularly application programing interfaces (APIS). The main objective of this paper is to provide guidance on how to implement consumer consent protocols to access bank account data under open banking scenarios.

Digital financial services are creating opportunities to accelerate financial inclusion, closing the gap in access that has long existed, especially for low-income and rural consumers. In many instances, new non-bank providers of financial services are entering these markets, leveraging their proximity to previously unbanked customers and the data they have. Mobile network operators are perhaps the best known of the non-bank providers of digital financial services, but many others are in both the payment space and other areas, such as credit (peer-to-peer lending or cash-flow lending on e-commerce platforms), microinsurance, or firms offering to optimize their clients' use of financial services.

In a bank-centric financial system, large institutions are responsible for managing customer data and, in many cases, share a limited amount of consumer data with third parties. As non-banks enter financial markets, consumer account data—including data from the banking system—is necessary to provide additional and more efficient services as well as custom-tailored products.

Open-banking schemes provide consumers with more choice and new financial products and services through the use of technology, particularly application programming interfaces, which enable smooth access to consumer data, allowing third parties to provide services that require such data (payments, for instance) without the need to collect or store the information. A key element of open banking is the sharing of the consumer's personal data, including financial information, with a third party or parties. In essence, this initiative is opening the traditional banking and finance sector to new participants, with the objective of increasing competition and innovation.

To date, over 22 jurisdictions around the world have either implemented an open-banking initiative or are working toward it. Jurisdictions have adopted different schemes that vary in scope and requirements, including governance, types and number of participants, type of data accessed, type of access to data (read or write), and technological solutions to the access. However, a common challenge in all jurisdictions is the enabling of *permissioned* customer data access to third parties.

This report focuses on the issue of consumer consent in open banking, highlighting the jurisprudence in both the European Union, which serves as a model for many countries globally, and a select group of countries: Australia, Brazil, India, Mexico, and Rwanda. The report provides practical insights into how to implement consent mechanisms under an open-banking scheme.

1

INTRODUCTION

Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, including, for example, those that provide real-time payments, greater financial transparency options for account holders, marketing, and cross-selling opportunities.[1]

In effect, open banking is opening broader access to bank data.[2] Some authors define it as "a standardized sharing of data and services through the opening and integration of systems" (Plaitakis and Staschen 2020). This access to, and sharing of, customer data by banks and other financial institutions that hold customer accounts with third-party providers (TPPs) is sometimes mandated by law—and customer consent is a central feature.

Open banking was developed to encourage innovation in financial products and services and expand choice for consumers by breaking down barriers to competition arising from unequal access to customer information. The traditional banking system is based on the exclusive use of customer data for payments, investments, and money management generally; only limited types of data, such as repayment of loans, are shared with third parties.

Open banking is a model developed in the last decade to allow third parties access to information held by banks with the permission of the customer. The European Union's revised Payment Services Directive (PSD2) and its forerunner, PSD1, are the basis for open banking. In 2016, the Competition and Markets Authority published a report on the United Kingdom's retail banking market that observed that smaller and newer banks found it difficult to grow and access the market, while existing, and particularly larger, banks do not face adequate competition. This main observation—which affected a market composed of 70 million active personal accounts[3] and 5.5 million business accounts—is based on the assumption that a large percentage of personal account holders would gain from switching to cheaper products. Traditionally, banks have been in control of the data of their customers and operate within a closed architecture that allows them to make use of such data and gives them a built-in advantage on the design and development of products and services offered to their clients.

One of the main legal restrictions on banks' ability to share data with third parties is the existence of bank-secrecy provisions that establish the duty of confidentiality on banks toward their clients. Violation of bank secrecy in many jurisdictions is considered a criminal offense, and bank officials are therefore cautious about disclosing their clients' information with third parties. However, these provisions are not absolute and are subject to exemptions—a common exemption relates to the prevention of money laundering and financial terrorism and to the monitoring of credit risk. Another exemption to bank secrecy recognized under the famous *Tournier v. Bank of England* case *is based upon the customer's consent.*[4] Open banking also creates an exception to bank-secrecy protections, based upon customer consent, with the objective of benefiting consumers by enabling third-party[5] access to account data held by banks.

Since rules under an open-banking scheme are enacted by different authorities, potential conflicts of law may

exist. In addition, one of the objectives of enabling open banking is to provide consumers more control over their account information and the possibility to decide with whom they would like to share such data to obtain additional and more convenient and attractive products or services. In such a context, the consumer's consent to allow third parties access to information through application programming interfaces (APIs) has become a key issue in the formulation of the legal and regulatory framework of open banking. This document aims to explore practical solutions to the provision of consent, taking into consideration existing laws while also making use of technological solutions to address the need for customers' permissioned access to their data. There are several perspectives to consider regarding why the authorization of the customer is necessary under open-banking schemes: (i) requirements of a contractual nature in relation to the access to, and subsequent processing and storage of, personal data for the purpose of providing payment services; (ii) explicit consent in line with article 6 of the General Data Protection Regulation (GDPR); and (iii) consent to allow access to a customer's banking data as per bank-secrecy provisions (EDPB 2020a). The objective of the consent mechanism is not to solve all measures related to the data-protection framework but to provide for a framework that translates permissioned access into the enabling technology.

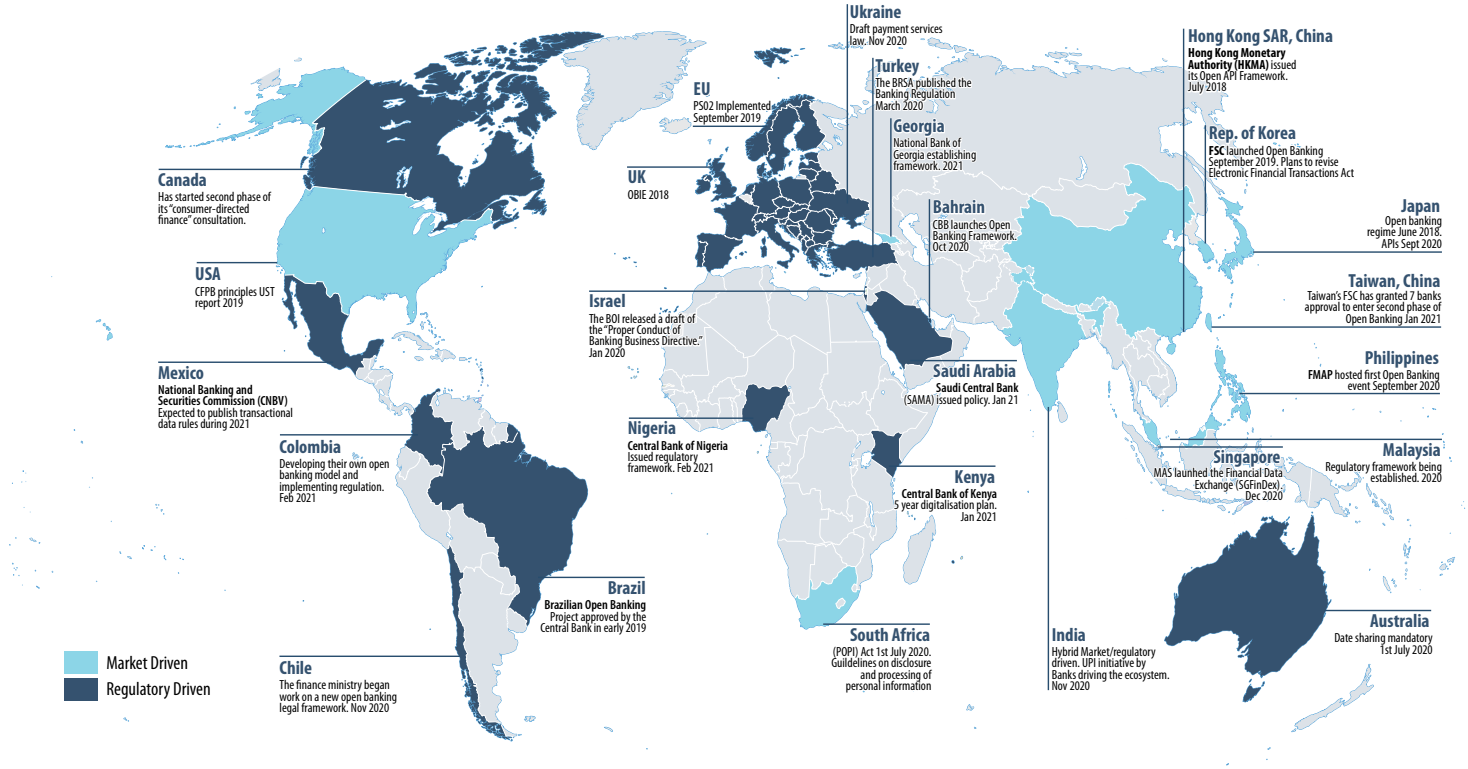
While open banking increases transparency in financial markets by making data more widely shared, it also creates concerns about personal data protection and privacy. Explicit consent addresses the inherent tension that exists in the use of personal data for commercial purposes—such as open banking—by enabling consumers to exert control over the use of their data. This approach also reflects the legal approach to privacy for individuals compared to firms—people are recognized to have a right to privacy, while firms are not.[6] In many jurisdictions, personal data-protection regimes are part of the broader legal framework for open banking and often based on another well-known European benchmark—the GDPR.

The potential for open banking is great; according to projections by Allied Market Research, the global open-banking market will grow at an estimated annual rate of nearly 25 percent between 2019 and 2026, going from $7.2 billion in 2018 to over $43 billion by 2026.[7] Millions of consumers are already benefitting from open banking. South Korea is a particular standout; 20 million consumers have used open-banking services—approximately 70 percent of the economically active population—in just the first two years of such services becoming available (since 2019).[8] South Korea is an outlier in the speed of adoption—other countries, such as the United Kingdom and India, each have fewer than five million open-banking customers as of 2020—but Korea's experience shows the potential for open banking when conditions are right. Notable features of open banking in Korea include a strong regulatory framework and joint platform that doesn't require bilateral partnerships between banks and TPPs; the ability of both large and small fintechs to use the system to promote innovation and competition; functionality, including the ability to use open banking for wire transfers; and a very high penetration of smartphones (over 90 percent of the population).[9]

The promise of open banking for financial inclusion is potentially transformational, as it would allow not only access to new customers but also the offer of new products and services to existing ones. By harnessing data from a range of financial providers and commercial firms, which may include fintechs and other technology companies, retailers, and utilities, open banking reduces information asymmetries, opens doors for new innovative products and services, and increases competition. However, obtaining the benefits of open banking for financial inclusion requires intentional design of policies and products, which, so far, is uneven across jurisdictions. Research by the Consultative Group to Assist the Poor identifies Brazil, Indonesia, and Mexico as three countries that have been proactive in leveraging open banking to increase financial inclusion (Plaitakis and Staschen 2020).

While initial open-banking developments took place in the European Union and United Kingdom, as of June 2021 a number of countries are already implementing open banking in Asia, the Americas, and, to a lesser extent, Central Europe. Only two countries have developed open-banking initiatives thus far in Africa. The spread of open banking beyond Europe can be seen in figure 1, which was produced for the Basel Committee on Banking Supervision's 2019 publication *Report on Open Banking and Application Programming Interfaces*. The following jurisdictions have currently implemented or are in the process of implementing an open-banking scheme: Australia, Brazil, Chile, Colombia, the Czech Republic, the European Union, Georgia, Hong Kong, India, Israel, Japan, Mexico, Singapore, Turkey, the United Kingdom, and Uruguay. The United States launched an open-banking report and Malaysia an open-banking policy document. Nigeria released an open-banking framework just in May 2021, and Rwanda issued open-banking regulations in 2018. Indonesia issued the payment systems playbook, and China has not yet issued a policy document on open banking, but the fintech industry is driving efforts on open banking. The Philippines is currently developing the regulatory framework on opening banking, while

FIGURE 1: Open-Banking Developments Globally



Source: Konsentus, July 2021

Israel released draft guidelines for credit card companies and banks to allow non-bank financial institutions access to their data for payment services. Turkey started with the amendment of the payment systems and e-money institutions law and their main legal text for open banking, although the banking law explicitly recognized the open-banking services and included services broader than just payments (that is, remote identity-verification services). In all of these economies, consent is part of the legal and regulatory approach to open banking, providing a mechanism to protect consumers from unwanted disclosures of personal data or overly aggressive digital marketing, and to help justify greater transparency in financial markets as something driven by consumer demand.

While consent is a core part of the legal and regulatory framework for open banking, clear guidance on how to implement consent is frequently lacking. Data-protection laws provide general requirements on consent clauses but may not fully reflect the technology and market conditions present in open banking.

The main objective of this paper is to provide guidance on how to provide consent under open-banking scenarios. It is important to clarify that the intention is not to cover all the necessary protective measures that are addressed through broader data-protection, governance, and cybersecurity frameworks. The authors also acknowledge that consumer consent under the GDPR and similar data-protection frameworks is not the same as that envisioned under PSD2, although the concepts are not contradictory. The objective of this document is not to discuss these additional scenarios and the potential risks of personal data sharing in general but to focus on permissioned access to data for either payment-initiation services or other related services based on account information. The range of data-protection and privacy considerations under data-sharing scenarios includes data-protection principles,[10] data governance and enforcement, and data security, including cybersecurity, which fall out of the scope of this document. By the same token, the usage of data for artificial intelligence and potential negative consequences resulting from data analytics and algorithm development are part of a broader discussion and not the object of this paper. Aspects related to "silent-party" data under an open-banking scheme are also not subject to discussion in this paper, which aims at explaining in greater detail pragmatic solutions to the need for operat-

ing under a customer-permissioned environment. Finally, authors acknowledge that the term *open banking is evolving, and some jurisdictions are embracing open finance and even open data beyond the financial sector. These developments are at a very preliminary stage, and it is too early to draw any conclusions—thus, they are also beyond the scope of this paper.*

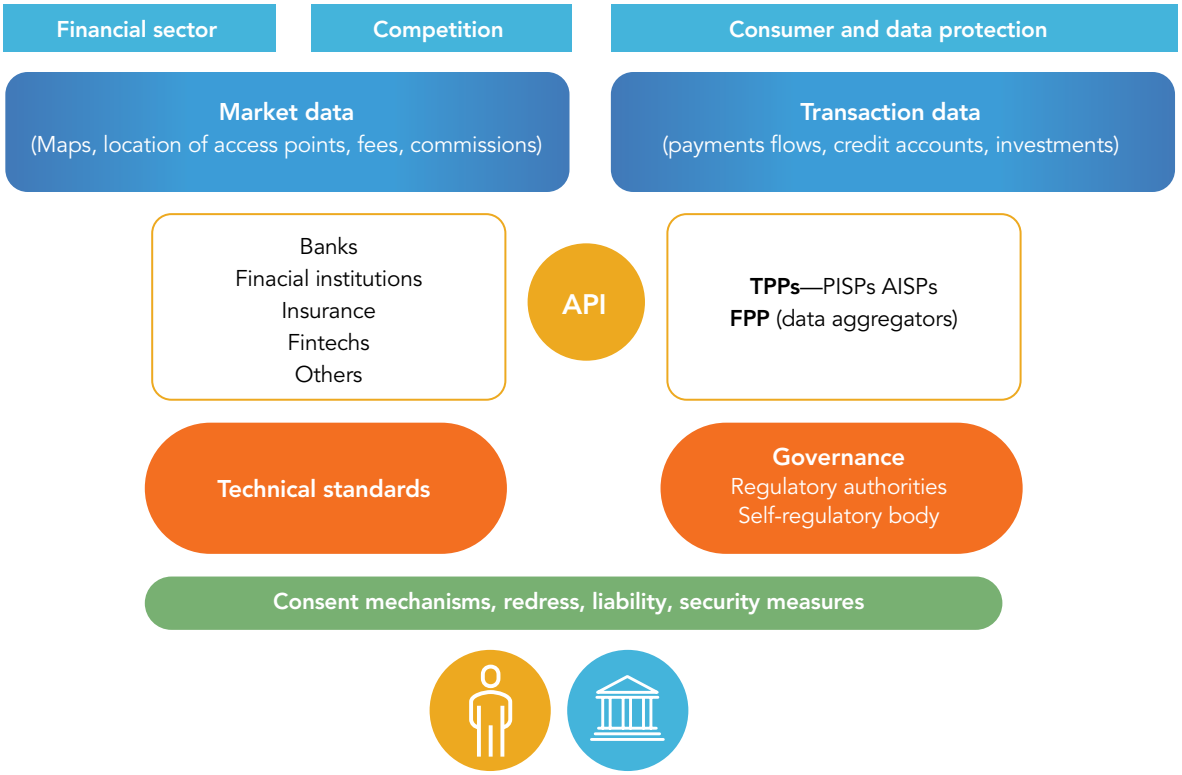
This report also briefly discusses the limits on consent as a way to protect consumers from abuse and identifies other actions regulators can take to balance innovation and transparency with privacy in a digital marketplace, in sections 2 and 3 of this report. Implementation options to consent, such as establishing a fiduciary standard for open-banking providers to meet, are briefly discussed, but in-depth treatment of these approaches is beyond the scope of this report.

A BRIEF INTRODUCTION TO OPEN BANKING

Open-banking schemes involve different authorities, market participants, types of data, technology, standards, rules, and governance schemes. (See figure 2.) The design of each open-banking scheme differs from one country to another, including the mandatory versus voluntary rules. However, even under mandatory schemes, the consent of the customer is required. This is different, for example, than for credit reporting, where participation is mandatory to protect credit quality and the soundness of the financial system. Under credit-reporting scenarios for credit data, the legitimate interest for data processing remains with the bank or credit provider in connection with overindebtedness and financial stability. However, under open-banking schemes, the main objective is not to evaluate the creditworthiness of the customer but to offer additional options to the consumer; therefore, the control and legitimate interest remains with the consumer. Since the benefit is intended to accrue especially to the customers, their permission is central to the transaction and provides part of the rationale for increased transparency. In addition, enabling consumers' permission to access their own account data by third parties allows the implementation of the data-portability concept, which is a key concept to increase market competition on financial services.

Data flows under open-banking schemes take place between a few relevant actors, including payment-initiation service providers (PISPs)[11] and account-information service providers (AISPs).[12] The role of the account-ser-

FIGURE 2: Open-Banking Ecosystem

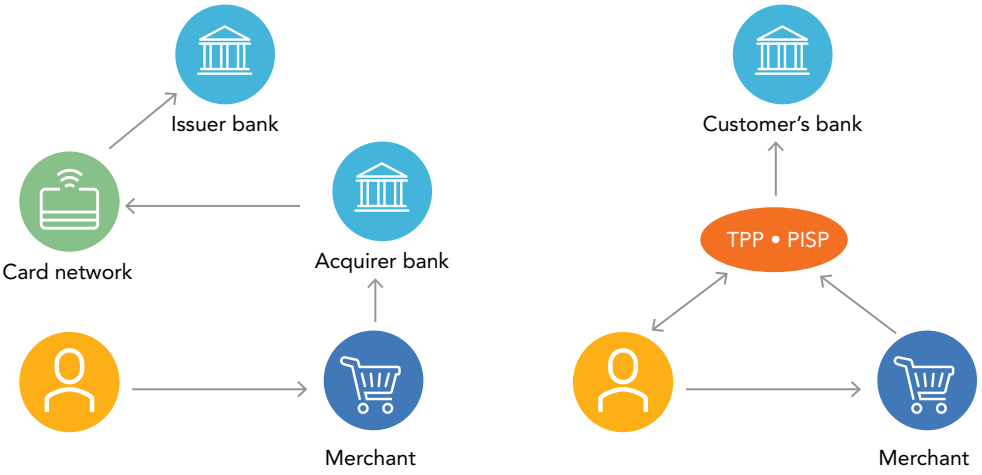


Source: World Bank (2020)

vicing payment service provider[13] has also been recognized under some jurisdictions. While under open-finance schemes, authorities are evaluating complexities of involving third parties and may be considering implications of reciprocity, it is important to understand that the obligation relies on enabling access and not necessarily proactively sharing the data with third parties. Therefore, most of the schemes put emphasis on the establishment of APIs and harmonization languages to enable data sharing between different parties and not necessarily on the actual data-sharing (sending-data) obligation.

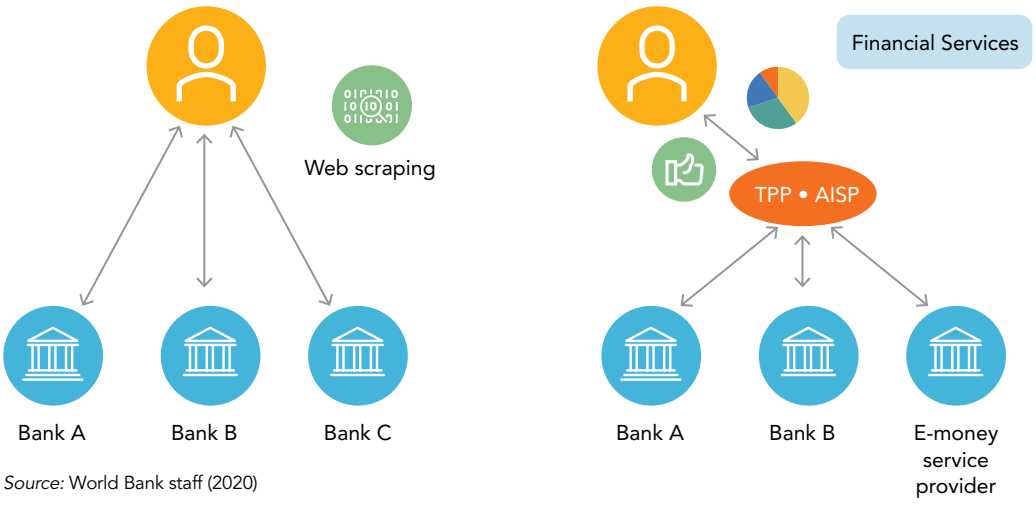
Open banking can securely provide other financial institutions and TPPs with seamless access to customer data through APIs. Several methods are used to access customer information, which can pose risks to customer data. Web scraping refers to a computer program or bot that extracts human-readable data (as email addresses, phone numbers, shopping behaviors, and more) from another program, site, or platform. In the context of online banking, for example, this means viewing the account balance, but bank customers must grant the service provider (the PISP) permission to access their banking data. For this purpose, they log onto the provider's platform using their online banking data (for example, sharing username and password with third parties). The reverse-engineering method allows access to the source code of an application, the insight view of the architecture, and the third-party dependencies. This method is considered a serious vulnerability in mobile applications and may cause a great

FIGURE 3: PISPs before and after Open Banking



Source: World Bank staff (2020)

FIGURE 4: AISPs before and after Open Banking



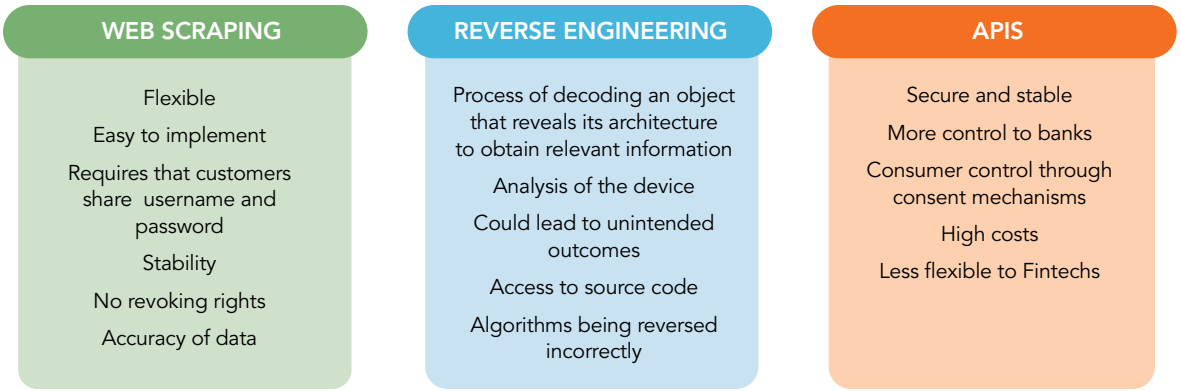
Source: World Bank staff (2020)

impact on the consumer as well as the bank. This information can further be used to upgrade, make a copy, or pursue any other malicious purpose. The big change with open banking is moving away from insecure screen scraping and password sharing to APIs. APIs,[14] on the contrary, provide a secure and standardized way for applications to work with each other and deliver the information or functionality requested. For the "API call," it is necessary to enable the customer permission/consent.

The primary audience for this report is financial regulators who are charged with the oversight and implementation of open-banking regulations, as well as regulators from other agencies who may also have jurisdiction due to the use of consumer data for financial services. These include telecommunications and utilities regulators and authorities responsible for consumer protection and data protection, depending upon the national regulatory structure. Other relevant audiences include private-sector financial providers engaging, or planning to engage, in open banking and development practitioners supporting digital finance, open banking, consumer protection, and data protection.

The remainder of this report is organized as follows. Section 2 briefly discusses the economics of information in financial markets, to provide a high-level overview of changes in the use and availability of information by financial services providers and the importance of willing customer participation in these systems. Section 3 discusses arguments for alternative approaches to consumer consent. Section 4 focuses on the foundational laws for open banking and consent that are used widely as guides for laws in other countries: PSD2 and the GDPR. Country cases are presented in section 5.

FIGURE 5: Scraping and Reverse Engineering versus APIs



Source: Presentation by World Bank staff at the Financial Inclusion Global Initiative Symposium (2021)

NOTES

1. Definition as per BCBS (2019).
2. The term is thought to have emanated from a United Kingdom initiative launched by the Open Banking Working Group to explore ways in which greater financial data access could assist consumers to understand their finances and make more-informed choices. The resulting UK Open Banking Standard relies on data being securely shared or openly published through open APIs that would let third parties, such as fintech companies, access users' data through their bank accounts. See ODI and Fingleton (2019).
3. Personal customer accounts allow for making and receiving payments with or without using cash or storing of money. Most personal accounts also offer a facility to borrow money on a flexible short-term basis. Seven percent of these accounts in the United Kingdom are basic accounts.
4. "It is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer express or implied, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, unless the banker is compelled to do so by order of a Court, or the circumstances give rise to a public duty of disclosure, or the protection of the banker's own interests requires it." In Tournier, the bank's duty of confidentiality extends to all information from account transactions.
5. It should be noted that not every third party under an open-banking scheme is allowed to access a consumer's data. Rather, only those that have been approved by the data-governance body of the open-banking scheme are allowed to do so.
6. In many instances, where the focus is on firms, especially those which are publicly held, the objective of law is how to achieve transparency.
7. Gill and Sumant, 2020.
8. Hamilton, 2019.
9. Financial Services Commission, open-banking resources, https://www.fsc.go.kr/eng/po030101; and Statista for smartphone coverage data, https://www.statista.com/statistics/777726/south-korea-smartphone-ownership/.
10. Lawful-basis processing, purpose limitation, and data minimization.
11. Refers to the provider of a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
12. Means a provider of an online service providing consolidated information about one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider.
13. Refers to a payment service provider providing and maintaining a payment account for payers, which are usually banks.
14. Please note that, depending on the type of API, the assets shared are more restrictive than private APIs.

2

THE ECONOMICS OF INFORMATION IN FINANCIAL MARKETS

The collection and analysis of customer information has traditionally been viewed as a key role of financial institutions. Through transaction accounts with consumers as well as other products and services, including credit, savings, and payment activities, financial institutions have access to a unique set of information about both the ability and willingness of borrowers to repay obligations, addressing issues of both adverse selection and moral hazard (Jaffee and Russell 1976; Stiglitz and Weiss 1981). These data can also be used to identify new sales and cross-marketing opportunities and to devise customer retention and collection strategies. AISPs present opportunities to enable additional services based on account information from banks and other financial institutions. The information gains even greater predictive power through analytical tools and statistical modeling, frequently referred to as credit scoring, which enables financial providers to quantify risks and adjust prices and policies accordingly (Barron and Staten 2003). This helps to reduce the impact of asymmetric information on financial markets, which can result in credit rationing and underdevelopment of finance more generally. In the absence of information sharing, large financial institutions have an advantage over smaller ones, as they can leverage data from many customers to strengthen empirical models and also have the resources to invest in these technologies.

Credit-reporting systems were developed to reduce further the impact of asymmetric information on financial markets by creating a mechanism for sharing information about customers—both individuals and firms—through centralized databases that include data from a number of financial services providers (Miller 2003). In some cases, credit-reporting data from financial institutions are complemented with data from other sources, including retailers that provide credit, utility companies, and public databases and registries. While consent clauses are often included in financial contracts to support data sharing with credit-reporting agencies, another rationale is based upon the public interest. Borrowers are viewed as having the obligation to share data on their loan performance to both monitor and incentivize good credit behavior and thereby reduce the risk of default and loss of funds for depositors. This obligation is limited, though, to regulated financial institutions and information related to existing or past repayment obligations or credit operations.

The transformation of many economic activities to digital platforms and channels that create enormous quantities of data on customer preferences, behavior, and financial activities—especially in terms of digital payments—are behind many innovative new fintech business models. E-commerce platforms have also leveraged data from transactions on their platforms to offer credit to small businesses.

Under open-banking schemes, PISPs are authorized to initiate payments into or out of a user's account without direct contact with their banks. PISPs are authorized to make transfers on behalf of customers, rather than only displaying account results. PISPs do this by using the bank's own resources to initiate transactions either to or from the payer's bank account. As a result of this type of action, PISPs have "read-write" access. The adoption of

open-banking schemes also presents opportunities for e-commerce, such as (i) reduced fraud rates in the industry and increased trust with consumers; (ii) increased online banking and payment options for e-commerce consumers; and (iii) merchants can leverage new payment aggregators to increase their strategic information on consumers.

As more nonfinancial sources of data are used to understand financial behaviors, data protection and privacy have gained even greater importance in the context of data sharing for finance. By helping to build trust and a sense of control among consumers, data protection and privacy safeguards, including consent, can increase the uptake and use of digital financial products and strengthen the formal economy. Clauses in data-protection and privacy regulations that establish time limits for the use of personal data can give consumers with negative performance episodes incentives to improve their standing, reducing the possibility that some consumers may become economically marginalized for temporary problems. Consent can also provide an opportunity to teach consumers about their rights and responsibilities in financial markets and with respect to data use, so they are better self-advocates and can help to enforce regulatory requirements and market discipline. Consent also creates the potential for tailoring the use of personal data to the needs of the individual, thereby minimizing negative externalities while working toward greater market transparency.

However, there are also important limitations to the use of consent as traditionally understood in other scenarios. According to researchers from Carnegie Mellon, it would take 76 days for an average consumer to read just the privacy and consent forms for web-based activities typically conducted during a year (Madrigal 2012; McDonald et al. 2009). If consumers read these documents (and they often don't), they are likely to have difficulties understanding them, even if the consumers are literate and educated, due to the documents' legalistic language. Small font sizes and formats that make it difficult to identify key data or topics quickly also contribute to consent being of limited use to consumers in many cases. Too often, consent boxes are simply ticked without any review, as consumers see them as essentially required in exchange for the use of the product or service.

Consent alone is inadequate to support data protection and privacy, but it is a critical tool that gives consumers some control over their data, if properly designed and implemented. The next section of the report discusses consent and alternatives and is followed by an analysis of consent as laid out in PSD2 and the GDPR. Section 4 also includes a discussion of the specific aspects of the design of consent that can strengthen its effectiveness for consumers, based on guidance related to implementation of the GDPR.

3

CONSENT AND ALTERNATIVES TO CONSENT

Open-banking regulations are designed to encourage the seamless sharing of data as part of improving competition and encouraging innovation in the financial-services sector. Part of the reforms introduced by PSD2 in the European Union give TPPs access to a customer's payment account data, assuming the customer provides the required consent. Other open-banking regulations (for example, those in Australia, Brazil, and India) clearly establish a consent protocol to access customer data, including additional safeguards such as limited access to accredited institutions, adopting data-protection measures in addition to consent, and enabling an oversight framework and data-governance structure, among others. That seems to be a straightforward approach, but as the analysis in this paper shows, there are many issues relating to consent, including its legal nature, and to the interplay between open-banking regulation and other regulation, especially data-protection and privacy laws and regulations.

Open banking is an economic reform, but it is based on processing personal data, with consumer consent. The use of such data could vary from enabling TPPs to provide payment-initiation services to comparators that use account information to compare services and products offered to a specific consumer from different service providers. While the confidentiality of information is very relevant, the focus on open banking has shifted on how consumers are able to control and maximize the beneficial use of their banking data (Leong 2020). As the European Data Protection Board (EDPB) observes, "If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing" (EDPB 2020b).

There are reasons to believe that the traditional way of providing consent through paper-based or electronic forms has some limitations. Therefore, this paper analyzes new forms of obtaining consent from consumers that provide them with broader control over their data as well as increased transparency from data controllers. As discussed earlier in this report, research has shown that the burden on consumers for reading privacy policies is great. In work done more than a decade ago, in 2008, researchers at Carnegie Mellon estimated that it would take 76 working days to read online privacy policies that correspond to typical internet use (McDonald et al. 2009). With even more online and digital commerce and activities today, this burden would seem more likely to have increased than decreased. Many consumers simply tick boxes or provide other required forms of consent without really understanding what they are agreeing to or the implications (Murthy and Medine 2018). The practical guidance provided in this report, and in other publications (Boyd and Hanouch 2021; Murthy and Medine 2018), on how to make consent more rigorous and effective can strengthen consent requirements, but fatigue with disclosures and consent agreements may reduce the impact of even the best-designed interventions.

Consent should be seen as one part of a more comprehensive approach to protecting consumers' interests; an adequate data- and consumer-protection framework is necessary to protect consumers effectively under open-banking schemes. In some instances, these involve consumer input, supervision, and feedback. In others, they relate to the "privacy architecture" built into financial products and services, of which consumers may not ever be aware.

In a related vein, privacy notices that lay out the terms and conditions for treatment of consumer data, and that are required by law and/or regulation, can create the basis for regulatory supervision and enforcement. While these notices may not be used directly by consumers, even though they would be publicly available, they are valuable both for regulators and for setting industry-wide expectations of behavior.

Developing a role for "learned intermediaries" who could audit the privacy policies in open banking and other providers of digital financial services and identify misuse of data or gaps in consumer protection has also been raised as a way to strengthen data protection. As with regulatory oversight, the advantage is that skilled professionals would engage in a review of data-protection and privacy policies and their effective implementation in providers. Rather than waiting for problems to come to light and harm to come to consumers, this kind of audit and supervision activity could complement other regulatory actions and help to identify and correct problems proactively. The governance arrangements adopted withing the open-banking schemes could take into consideration the adoption of mechanisms that are based on the concept of "privacy by design." Therefore, the collaboration between data-protection authorities and financial-sector regulators could be necessary when implementing consent mechanisms for open-banking schemes.

The creation of online platforms that enable consumers to review their personal data sharing quickly, including what they have consented to, is another innovative approach designed to increase transparency and ultimately consumer control of their data. By creating a common location for information on consumer data, individuals would have a better understanding of what data they have shared, for how long, and with whom.

Using "legitimate purpose" as a requirement for access to and use of data is also an approach that has been employed effectively in the past—for example, in the context of the US Fair Credit Reporting Act and credit reporting. As with the example of the fiduciary standard, setting out a legitimate-purpose requirement puts the burden on financial providers to limit use of data to instances where they are creating value for consumers. In the context of the US Fair Credit Reporting Act, this includes monitoring credit performance and for fraud, but also for new credit offers that introduce competition into the marketplace.

In fact, there may yet be more to go back and learn from experiences with credit reporting and data protection and privacy as they apply to open banking. For example, adverse-action notifications are powerful for protecting consumers, because they highlight when data has been used and resulted in harm. In the case of credit reporting, this may be a rejection of a credit application or a higher interest rate on a loan that is provided. A similar adverse-action notification could be developed for open banking, so that consumers are informed when their data has resulted in a negative outcome that could relate to paying a higher price for a financial product, receiving a smaller line of credit, or outright exclusion from certain offers. The online platform for information on consumer data is similar in some ways to the reports that consumers can request from credit bureaus, where inquiries to their data in the bureau are identified, helping to identify fraudulent requests or other misuse.

4

THE ROLE OF CONSENT IN RECONCILING OPEN BANKING, PRIVACY, AND DATA-PROTECTION FRAMEWORKS

Open banking in its current form is a relatively recent development, having initially been approved by the European Union in 2015 and by the United Kingdom in 2018. Following this lead, similar legal frameworks are being established by other developed and developing nations in Africa, the Americas, and Asia, as governments seek to encourage open banking. Some nations are using a market-driven approach, whereby open banking is permitted but not specifically regulated and may or not be officially encouraged. This type of "wait-and-see" approach to regulation is likely to result in no firm requirements on consent until formal laws or regulations are issued. Other jurisdictions are actively encouraging the development of open banking, often through the release of open APIs and technical standards and/or guidelines, but are not mandating open banking. The focus on technical standards may or may not be accompanied by regulatory guidance on consumer-protection issues, such as consent. The third approach is based on regulatory statutes, whereby a nation enacts legislation to mandate open banking. Usually, law requires at least some financial institutions, typically the nation's largest banks, to share data with accredited third parties with the consent of the consumer. The analysis of consent in open banking in relation to PSD2 and the GDPR presented in this section, and the country case studies developed for this paper and presented in the next section, focus on countries with an open-banking regulation because it is the most widely used approach and because it requires the sharing of consumer data with third parties with consumer consent.

Most countries are modelling their open-banking initiatives on PSD2, which provides the legal basis for open banking in the European Union (European Union 2015). PSD2 influenced a similar regime that is in place in the United Kingdom[15] and that nations outside Europe have

BOX 1

Open-Banking Principles Will Be Extended to Energy and Telecommunications Sectors in Australia

Open banking is really about data, specifically consumer data, and its access and use by TPPs. Around the world, the banking and financial-services sector is the first sector where this data sharing is being encouraged and facilitated through government policy and legislation. It can extend to other sectors and eventually be economy-wide. This is perhaps most clearly articulated by Australia, where open banking is now being implemented, and it will be extended to the energy and telecommunications sectors, paving the way for an envisioned economy-wide rollout.

since adopted for their open-banking initiatives. PSD2 is a European regulation for electronic-payment services and includes the regulatory framework for open banking. Further, PSD2 was designed to strengthen competition, consumer protection, and innovation in the payments market and contribute to the development of new methods of payment and e-commerce. PSD2 was an early model that other countries could readily adopt, and as a result, its influence is pervasive. Most nations follow PSD2 in terms of its objective of economic reform through increasing competition and fostering innovation in the banking and finance sector. Most nations also follow the basic approach of PSD2 for consumer consent, as well as identity authentication and data-security requirements.

The same pattern of international adoption that is occurring with open banking occurred earlier in relation to data protection. Almost without exception, nations around the world follow, to some degree, the European Union's data-protection framework as now set out in the GDPR. This general similarity in data-protection requirements—including consent and other lawful grounds for data processing, in addition to the right to portability—is significant because open banking is being introduced, in many instances, in countries that have established data-protection legislation based on the European Union's data-protection model.[16]

Because the European Union's models for both open banking and data protection are the most widely followed around the world, they form the basis of the discussion of the key issues regarding open banking and consumer consent in this paper. PSD2 does intersect with other EU directives and regulations, including the Directive on Unfair Contract Terms in Consumer Contracts 93/13/EEC (Unfair Contract Terms Directive). Similarly, consumer law and the general law of contracts apply in other jurisdictions. However, while there are basic similarities in intent and sometimes in approach, there are considerable national differences. While consumer-protection law and contract law have peripheral relevance and will be referred to more narrowly in this paper, PSD2 and the GDPR are of most direct relevance to consumer consent to data processing in an open-banking context. For these reasons, the analysis in this paper starts with a detailed analysis of PSD2 and the GDPR as the key international model regulations applicable to open banking. Section 4 looks at a select group of countries that are in the process of implementing open banking and analyzes how they are addressing consent.

Reconciling Open-Banking Rules with Data Protection and Privacy

Open banking is market reform, and the legislation that enables it is banking law. The data-protection law is essentially human rights legislation that was originally conceived in the context of the protection of privacy in the technology era. Moreover, data-protection frameworks also recognize the right to data portability, allowing consumers more control over their data.

Access to customer data by third parties has occurred in the absence of APIs with the use of the widespread practices of screen scraping or reverse-engineering techniques, still prevalent in several markets. Some of the concerns associated with screen scraping and reverse engineering have to do with security and customer protection, stability, and the lack of revoking rights on the part of the customer. The Standing Senate Committee on Banking, Trade and Commerce of Canada paid particular attention to the advantages and disadvantages of open banking versus screen scraping.[17] According to the committee's report, Canadians have little control over their financial data, while the adoption of new banking technologies, such as data aggregation and robo advisors, requires that fintech companies access this data easily and seamlessly. Currently, these companies use screen scraping, whereby banking log-in credentials are used to extract customer financial and transactional data.

In the context of the European Union, implementing access to permissioned consumer data requires an analysis of not only PSD2 but also the GDPR and the subsequent guidance of the EDPB.[18] One of the objectives of the PSD2's technical standards was to put an end to the practice of screen scraping, long a point of contention for banks.

Both laws discuss the role of consent, but PSD2 provides less guidance on what would constitute the "explicit consent" that consumers need to provide to comply with data-protection and privacy regulations when they use services enabled through open banking. Instead, PSD2 relies on the GDPR for a description of the elements of explicit consent. Since the GDPR is not specific to open banking, however, there is scope for varying interpretations of the data-protection requirements. In the United Kingdom, as a result of a Treasury consultation on the implementation of PSD2, the information commissioner viewed open banking as a way in which individuals' rights to data portability under article 20 of the GDPR may be given practical effect and help financial institutions meet their data-portability obligations. The information com-

missioner also referred to the regulatory technical standards on strong customer authentication and secure communication that have been developed by the European Banking Authority.

While most of the jurisdictions that have developed an open-banking scheme already had a data-protection framework in place, some have amended the framework (that is, Australia) and others developed it later. Excepting the case of the United States, all advanced economies already had a data-protection framework in place. Regardless of countries where such a framework does not exist (for example, the United States), the scheme recognizes the need for a data-permissioned environment. In India, the lack of a data-protection framework was questioned by the courts and prompted its development in 2019, taking into consideration potential solutions to the challenges faced when implementing a know-your-customer platform, such as the consent manager and data fiduciary. Nigeria and Rwanda issued a payment regulation to allow PISPs to access bank data in 2019.

An important element of the regulatory framework of open banking is the existence of bank-secrecy provisions that prevent banks from sharing information with third parties. This is typically overlooked when discussing the legal and regulatory approaches. Attention is geared toward the data-protection and privacy framework, but the main driver to data-sharing permissioned environments is the existence of bank-secrecy provisions in most of the civil law jurisdictions, regardless if they are advanced or emerging market economies.

Open banking is based on access to consumer data held by banks and other financial institutions within the definition of "account servicing payment service provider"[19] in PSD2.[20] The basis of this access as expressed in PSD2 is the explicit consent of the consumer, but neither consent nor explicit consent is defined; rather, PSD2 defers to the data-protection laws in place in the European Union, notably the GDPR. Under PSD2, banks must allow TPPs to access customers' payment account data only provided that the TPPs have the "explicit consent" of the customer (articles 64, 76, and 94, PSD2). Under the GDPR, besides consent, there are other legal bases for data processing, including the performance of a contract. However, PSD2 increases the requirements for data processing included under the GDPR and clearly establishes the need to obtain consent. This approach is consistent with the banking laws that typically include bank-secrecy provisions and requires consumer consent to access customer data by third parties.

FIGURE 6: Legal Provisions Affecting Customer's Banking Data Sharing

COUNTRY	DATA PROTECTION	BANK SECRECY
Australia	Amended with CDR in 2019	NO
Brazil	2011 and amended in 2019	YES until 2019
Canada	PIPEDA	NO
Colombia	LPD 2012	YES (exceptions)
European Union	GDPR	Some had until 2018
Georgia	DPL 2012	NO
India	No, developed later DPA in 2019	NO
Indonesia	NO	YES
Malaysia	2010	YES
Mexico	2010	YES
New Zealand	1993	YES
Nigeria	Regulation	YES
Philippines	2012	YES
Rwanda	Developed in parallel 2019	NO
Singapore	2012	YES
Turkey	2016	YES
UK	DPA 1998	NO
US	Not comprehensive	NO; the Bank Secrecy act actually aims at the opposite

Source: World Bank staff elaborations using UNCTAD data (2020)

Article 64 of PSD2 establishes that (1) member states shall ensure that a payment transaction is considered to be authorized only if the payer has given consent to execute the payment transaction. A payment transaction may be authorized by the payer prior to or, if agreed between the payer and the payment service provider, after the execution of the payment transaction. (2) Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the PISP. In the absence of consent, a payment transaction shall be considered to be unauthorized. (3) Consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with article 80. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorized. (4) The procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s).

The AISP shall provide services only based on a payment service user's explicit consent. Article 67 establishes that member states shall ensure that a payment service user has the right to make use of services enabling access to account information. That right shall not apply where the payment account is not accessible online. The article also includes other measures to protect a consumer's data and limit the usage of such data by TPPs. These measures include the need for personalized credentials, identification for each communication session, secure communication between service provider and user, limits on the information to which access should be associated with the payment transaction, a prohibition to request sensitive payment data linked to the payment accounts, and limits on the purposes to access, process, and store data. In addition, the article also refers to conducting this service in accordance with data-protection rules.

Article 94 of PSD2 establishes that member states shall permit the processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation, and detection of payment fraud. This processing shall be carried out in accordance with the GDPR. Section 2 of article 94 establishes that payment service providers shall access, process, and retain personal data necessary only for the provision of their payment services, with the explicit consent of the payment service user.

Key Elements to Consider When Implementing Consent under Open-Banking Schemes

The essential requirements for valid consent under the GDPR are that the data subject's consent is freely given, specific, informed, and an unambiguous indication of the data subject's wishes by a clear affirmative action.[21] Article 7 of the GDPR sets out the following further conditions for consent: (i) the need to demonstrate that the data subject has consented to the processing of his or her personal data, (ii) the request for consent shall be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, and uses clear and plain language, and (iii) the right to withdraw his or her consent at any time; withdrawal shall be easy. (iv) When consent is conditional to the performance of a contract, the processing of personal data shall be limited to what is necessary for the performance of that contract.

SPECIFIC PURPOSE AND INFORMED CONSENT

Consumers shall be informed about the purpose of the processing, and who is ultimately responsible for such processing, so that they can make informed decisions, understand what they are agreeing to, and withdraw their consent. The EDPB establishes the following list of elements that are required for obtaining valid consent to the processing of personal information:

i. The controller's identity
ii. The purpose of each of the processing operations for which consent is sought
iii. What (type of) data will be collected and used
iv. The existence of the right to withdraw consent
v. Information about the use of the data for automated decision-making
vi. On the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in article 46[22]

The EDPB adds that, where the consent sought will be relied upon by multiple controllers, or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, all the controllers should be named. Processors, such as third parties used by AISPs and PISPs, do not need to be named as part of the consent requirements but to comply with articles 13 and 14 of the GDPR. Controllers have to provide a full list of recipients or categories of recipients, including processors. The

EDPB also notes that, depending on the circumstances and context, more information may be needed to allow the data subject to genuinely understand the processing operations at hand.[23]

Obtaining valid consent is therefore preceded by the determination of a specific, explicit, and legitimate purpose for the intended processing activity under article 5(1)(b) of the GDPR or article 94 of PSD2. As the EDPB and Article 29 Working Party (WP29) indicate, specific consent and the purpose limitation in article 5(1)(b) are safeguards to the gradual broadening or blurring of processing purposes, after a data subject has agreed to the initial collection of the data. "This phenomenon, also known as function creep, is a risk for data subjects, as it may result in unanticipated use of personal data by the controller or by third parties and in loss of data subject control" (EDPB 2020b).

CLEAR AND PLAIN LANGUAGE

The EDPB also states that, "when seeking consent, controllers should ensure that they use clear and plain language in all cases." This means a message should be easily understandable for the average person and not only for lawyers. Controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form. This requirement essentially means that information relevant for making informed decisions on whether to give consent may not be hidden in general terms and conditions. A controller must ensure that consent is provided on the basis of information that allows the data subjects to identify easily who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose of the data processing for which consent is requested" (EDPB 2020b). The EDPB says that if consent is to be given by electronic means, the request must be clear and concise, and the board notes that the controller must account for such factors as age in ensuring that the information is understandable, including how it is presented (EDPB 2020b).

CONSENT FREELY GIVEN

Consent under the GDPR is valid only if the data subject can make a real choice free from deception, intimidation, coercion, or significant negative consequences, such as substantial extra costs, if he or she does not consent. Consent is not freely given when "there is any element of compulsion, pressure or inability to exercise free will."[24] Furthermore, as the EDPB points out, "compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject's choices and stands in the way of free consent."[25]

Guidance from WP29 reinforces the role of article 7(4) in determining whether consent is freely given: "Article 7(4) GDPR plays an important role. Article 7(4) GDPR indicates that, inter alia, the situation of 'bundling' consent with acceptance of terms or conditions, or 'tying' the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is highly undesirable." If consent is given in this situation, it is presumed to be not freely given.[26] Article 7(4) seeks to ensure that the purpose of personal data processing is neither disguised nor bundled with the provision of a contract for a service for which these personal data are not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract.[27] The EDPB adds that the term "utmost account" in article 7(4) "suggests that special caution is needed from the controller when a contract (which could include the provision of a service) has a request for consent to process personal data tied to it."[28]

The GDPR makes clear that consent to the processing of personal data is not considered to be freely given if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment and where there is a clear power imbalance between the data subject and the controller.[29] Relating this to open banking, consent is unlikely to be regarded as freely given if the provision of the service is conditional on the data subject's consent to certain data-processing activities that are unnecessary for the performance of that service.[30] Consent must also relate to specific processing operations and should cover all processing activities.[31] The latter requirement is particularly important for open banking, especially if the processing has multiple purposes.[32] Consent is also presumed not to be freely given if separate consents are not permitted for different data processing when separate consents would be appropriate.[33]

While the GDPR lays down general principles regarding consent to the processing of personal data, there are many aspects to be considered when applying them to open banking. For example, is it clear that a consumer who consents to a payment service understands and consents to direct access to his or her banking account and that access may be via a party other than the AISP or

PISP? Does the consumer understand that he or she can limit the consent to access to specific data and can limit the data that is processed for the particular open-banking service? If the AISP or PISP as data controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, consent is neither free nor informed. As to explicit consent, although it is also not defined in the GDPR, recital 32 states that "silence, preticked boxes, or inactivity should not therefore constitute consent."

WITHDRAWAL OF CONSENT

A key element of consent is control by the data subject. Therefore, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment. As part of this control, under the GDPR the data subject has the right to withdraw consent at any time. Article 7(3) of the GDPR provides that "the data subject shall have the right to withdraw his or her consent at any time and such withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal."

The controller must ensure that consent can be withdrawn by the data subject as easily as giving consent and at any given time. In the view of the EDPB, when consent is obtained via electronic means through only one mouse click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of a device connected to the Internet of Things, or e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his or her consent without detriment. This means, among other things, that a controller must make withdrawal of consent possible free of charge or without lowering service levels."[34]

Article 64(3) of PSD2, however, states that the consumer's consent to the payment transaction may be withdrawn by the payer at any time but immediately qualifies this with a cut-off time limit designed to ensure efficiency in the payments system.[35] The right of the consumer to withdraw consent at any time is in line with the same right of the data subject under the GDPR in relation to the processing of personal data, but the cut-off time is not in line but justified by the specific needs of making payments efficiently.[36] The withdrawal of consent on open banking is similar to the revocation of authorization of automatic payments under a recurrent-payment service. This could be utility bills, card bills, car payments, gym fees, and so forth. Under those circumstances, there are also timelines (for example, three business days before the payment is scheduled).

EXPLICIT CONSENT

Consent, as required for part (a) of article 6(1), is defined in article 4(11) of the GDPR to mean "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[37] Explicit consent is not defined in the GDPR but is the subject of guidance from the EDPB: "The term explicit refers to the way consent is expressed by the data subject" (EDPB 2020b, 20). This explicit consent is different in nature to the explicit consent required under PSD2, which, according to the EDPB, is contractual consent allowing for lawful processing pursuant to ground (b) of article 6(1) of the GDPR. Explicit consent is required under the GDPR when the type of data or type of processing involves what is regarded as heightened risk, so a greater degree of control by the data subject is considered necessary. Explicit consent is required under article 9 for processing special categories of data, when processing involves international data transfer to a third country (in the absence of adequate safeguards) under article 49, and under article 22 for automated individual decision-making, including profiling.

The EDPB clarifies that explicit consent under the GDPR means that the data subject must give an express statement of consent. Under the GDPR, the consent does not necessarily have to be in writing. Explicit consent can be oral, albeit with the caveat that oral consent makes proof more difficult.[38] An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement (EDPB 2020b, 20–21). In guidance that is directly applicable to open banking, the EDPB states that, where appropriate, in the digital or online context, "a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature" (EDPB 2020b, 21). The EDPB continues, "A data controller may

also obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance 'I, hereby, consent to the processing of my data,' and not for instance, 'It is clear to me that my data will be processed.'"[39] Most significantly to open banking, the EDPB states that "a controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')."[40] Physical motions can constitute a clear affirmative action in compliance with the GDPR, in the opinion of the EDPB (EDPB 2020b, 19). However, in accordance with recital 32, in the view of the EDPB, action "such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action" (EDPB 2020b, 19). This is because it is difficult to differentiate this activity as unambiguous consent.

PSD2 uses two-stage verification of consent, and this is specifically supported by the EDPB as "a way to make sure explicit consent is valid." For example, a data subject receives an emailed notification of the controller's intent to process a record containing data. The controller explains in the email that it asks for consent for the use of a specific set of information for a specific purpose. If the data subject agrees to the use of this data, the controller asks him or her for an email reply containing the statement "I agree." After the reply is sent, the data subject receives a verification link that must be clicked, or an SMS message with a verification code, to confirm agreement (EDPB 2020b, 21).

The EDPB mentions a major issue for the digital era: click fatigue and the diminishing effect of online consent mechanisms. The board acknowledges that "this results in a situation where consent questions are no longer read. This is a particular risk to data subjects, as, typically, consent is asked for actions that are in principle unlawful without their consent." The EDPB notes that the GDPR "places upon controllers the obligation to develop ways to tackle this issue" (EDPB 2020b, 21). The opinion mentions the practice of obtaining the consent of internet users via their browser settings but says only that the consent must comply with the validity requirements set down in the GDPR for consent (EDPB 2020b, 19–20).

Section 5 discusses how a select group of countries have built upon the foundations provided by PSD2 and the GDPR to tackle the issue of consent for open banking.

NOTES

15. The United Kingdom's Open Banking regime is implemented through the Competition and Markets Authority's Retail Banking Market Investigation Order 2017, which requires the United Kingdom's nine largest banks, upon request from customers, to provide regulated providers access to the customer's banking data via a secure and standardized format.
16. The extent to which data-protection legislation is followed and enforced varies. Plaitakis and Staschen (2020) also highlight the links between data-protection regimes and the introduction of open banking.
17. https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_SS-11_Report_Final_E.pdf.
18. Please note that the EDPB was the former Article 29 Working Party that provides jurisprudence on data protection.
19. "Account servicing payment service provider" is defined as "a payment service provider providing and maintaining a payment account for a payer," but for ease of reference, this discussion continues to refer to these institutions as banks.
20. Article 4(17) of PSD2.
21. Article 4(11).
22. See EDPB (2020b), 15–16. This echoes the view of the WP29. See WP29 (2018), 13. See also recital 42 of the GDPR, which states: "Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. … A declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. sets out these requirements."
23. See EDPB (2020b), 16.
24. EDPB endorsing the opinions of the WP29. See EDPB (2020b), 9.
25. See EDPB (2020b), 10.

26. Recital 43 adds that consent is presumed not to be freely given if the process/procedure for obtaining consent allows data subjects to give consent for some processing but not for others.
27. WP29 (2018). The EDPB adds that "[I]f consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given." See EDPB (2020b), 7.
28. See EDPB (2020b), 11.
29. Recitals 42 and 43.
30. Article 7(4) and recital 43.
31. Recital 32 also states: "[C]onsent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them."
32. See recital 32.
33. Recital 43.
34. See EDPB (2020b), 23.
35. The moment of irrevocability in accordance with article 80. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction is considered to be unauthorized.
36. Articles 16–20 of the GDPR indicate in the case of withdrawal, when the processing is based on consent, the data subject has the right to erasure and the rights to restriction, rectification, and access. See EDPB (2020b), 32.
37. The GDPR places the onus on the data controller to demonstrate that the data subject's consent is informed and not coerced. The GDPR now clarifies that consent will be considered not to be freely given if the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment, and where there is a clear imbalance between the data subject and the controller, though this is particularly stated in relation to a public authority. See recitals 42 and 43 of the GDPR.
38. Under the GDPR, the burden of proof is on the data controller to establish that all conditions for valid explicit consent are met. Under PSD2, the PISP or AISP must similarly establish consumer consent. See articles 66 and 67.
39. "An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation)." See EDPB (2020b), 21.
40. "When consent is to be given following a request by electronic means, the request for consent should not be *unnecessarily* disruptive to the use of the service for which the consent is provided" (EDPB 2020b, 19).

5

COUNTRY CASE STUDIES

UNITED KINGDOM AND EUROPEAN UNION MODEL

The model on consent developed in the United Kingdom is valid for 90 days. The consent token expires and needs to be renewed. If a consent needs to be modified, the model allows to revoke the consent and provide a new consent. PSD2 mandates the European Banking Authority with developing regulatory technical standards on strong customer authentication and secure standards of communications among account-servicing payment service providers, PISPs, AISPs, payers, and payees. Commission Delegated Regulation (EU) 2018/389 supplementing PSD2 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication entered into force on March 14, 2018. The obligations set forth in the regulatory technical standards should apply since September 2019, although an extension has been provided to enable smaller institutions to adopt these rules. AISPs and PISPs need to develop mechanisms for consumers to see their consents provided and revoke them easily. Dashboards are presented to inform consumers about the status of consent with different TPPs, and, in addition, consumers receive confirmation emails of consent provided to the TPPs.

Below is an example of a consent mechanism that was developed by WSO2 and is compatible with regulation on open banking and data protection in the United Kingdom and European Union. It specifies the following: (i) to whom they are granting rights (TPP identity); (ii) for what purpose (payment/account details); (iii) for what period of time (number of days); and (iv) expiration process (when it will expire and how the user can revoke consent—typically 90 days if not revoked by the consumer). The process entails consent, authorization, and authentication.

Phase 1: Consent

In the consent phase, the interface shows the user what information is requested and for what purposes. The user can opt out, and sufficient information is available about the time-bound permission. This phase will be utilized by both the TPP and banking interfaces. It is in the TPP interface where the customer is first provided with the consent details to which he or she is going to provide consent. When it comes to the banking backend, the consumer must first be authorized by the bank to provide the consent details.

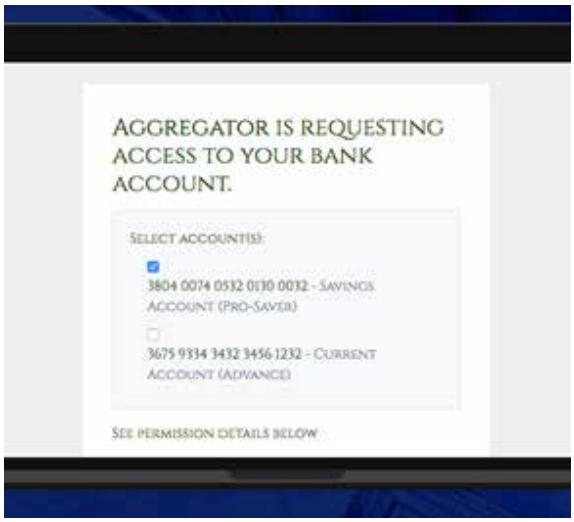
Phase 2: Authentication

After the user is informed about providing consent, it is the bank's responsibility to take over and provide the user within authentication mechanisms to ensure the security of the customer's data.

Phase 3: Authorization

Finally, the consumer is presented with the details about the consent required on the bank-user interface and is asked to allow or deny the TPP's request to access the data shown. The user's response needs to be recorded and stored.

Phase 1: Consent



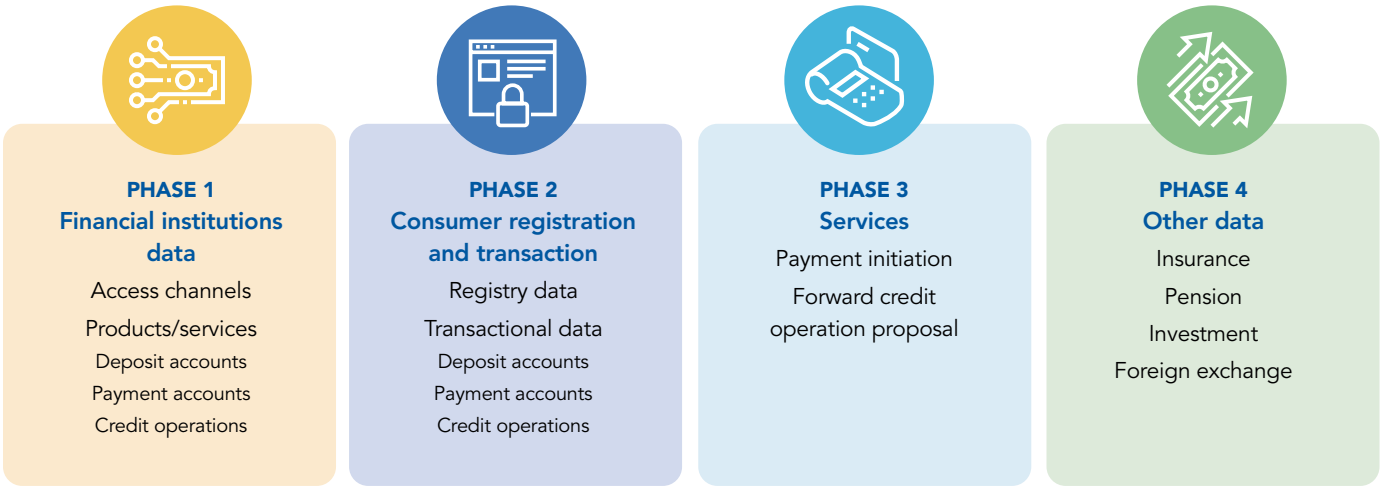
Phase 2: Authentication

THE SITUATION IN BRAZIL

In Brazil, the Central Bank of Brazil's Regulation on Open Banking, Joint Resolution No. 1 of May 4, 2020,[41] (Joint Resolution) entered into force on June 1, 2020. The joint resolution sets out a timetable for phasing in open banking. The first phase for sharing data on service channels, products, and services was to be completed by February 1, 2021, and full implementation of all phases is to be completed by December 15, 2021—dates that were slightly extended from initial plans due to the COVID-19 pandemic.[42] The joint resolution provides for the implementation of open banking by financial institutions, payment institutions, and other institutions licensed by the Central Bank of Brazil. Article 6, part I(a), makes participation mandatory for banks, and required sharing is extensive.[43] The joint resolution contains provisions that facilitate timely and efficient sharing by these institutions, including a prohibition on such impediments as setting up obstacles or limits on sharing.[44]

The stated open-banking objectives are to encourage innovation, promote competition, and increase the efficiency of the national financial system and the Brazilian payments system, promoting financial citizenship.[45] In fulfilling the objectives, the regulation requires that account service providers, data-transmitting institutions, data-recipient institutions, and PISPs pursue their activities ethically and responsibly, in observance of the legal and regulatory framework and observing the principles of transparency, security and privacy of the data and services shared within the scope of the joint resolution,

FIGURE 7: Phased Approach to Open Banking in Brazil



Source: Banco Central do Brasil

data quality, nondiscriminatory treatment, reciprocity, and interoperability.[46] Article 31 of the resolution states that participating institutions are responsible for ensuring the reliability, integrity, availability, security, and confidentiality with respect to the data and services sharing . . . as well as for compliance with the legal and regulatory framework in effect.[47] Consent must be obtained from the customer[48] under article 10 for customer registration and transactional data and for specified services related to the customer.[49]

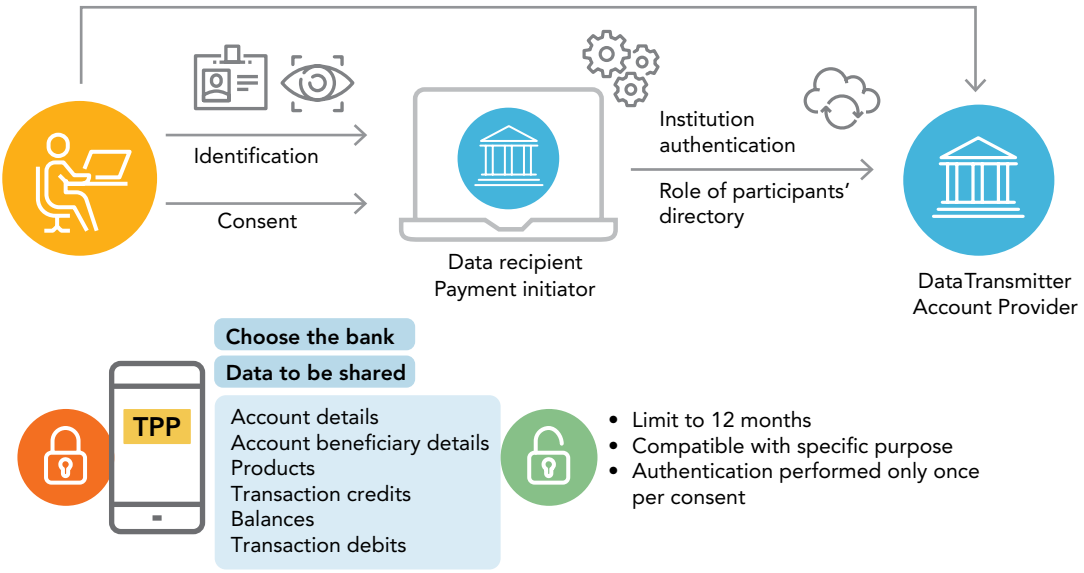
Registration data includes data provided directly by the customer or obtained by consulting public or private databases, and it must be the most recent data available, specifying the date that it was obtained.[50] Sensitive personal data, credit scores or ratings, and credentials and other information used with the objective of authenticating the customer are specifically excluded. Transaction data is data pertaining to the customer about products and services contracted with or distributed by the data-transmitter institution and accessible through its electronic service channels, including "pre-approved credit limits eventually agreed." At "a minimum, the data and transaction history of the past 12 months with respect to the products and services with valid contracts within that period" must be included.[51]

Open banking in Brazil must comply with the General Personal Data Protection Law (*Lei Geral de Proteção de Dados Pessoais, LGPD*),[52] which creates a new legal framework for the use and protection of personal data in Brazil by the private and public sectors. The legislation went into immediate effect in September 2020, but penalties will not begin to be levied until August 2021.

The LGPD follows the European Union's GDPR closely, including its definitions of personal data, sensitive personal data, and requirements for data processing that generally apply to the customer data used for open banking. The right to data portability is also included, which is seen as a major step in fostering competition because it allows consumers to transfer their data to other providers. The LGPD replicates the GDPR exactly in relation to consent and the other non-consent legal grounds for data processing. The GDPR has six lawful bases for that processing, while the LGPD has 10 grounds, but the LGPD grounds generally do not differ substantially from those in the GDPR, with an important exception: The LGPD allows data processing "for the protection of credit, including with respect to the provisions of the applicable law."[53] This is a significant departure from the GDPR, and it substantially broadens the possibility for lawful data processing in Brazil without consumer consent.

The open-banking joint resolution includes detailed provisions on consent in line with the European Union's model based on consent, authentication, and confirmation. Article 8 establishes that the request for sharing this registration and transactional data and services comprises the stages of consent, authentication, and confirmation. Consent is defined as "a free, informed, previous and unequivocal manifestation of will, made through electronic channels, by which a customer agrees to the sharing of data or services for specific purposes." A data-recipient institution or PISP must identify the customer and obtain his or her consent prior to the sharing. The consent must be requested using clear, objective, and suitable language; refer to specific purposes;[54] have a validity period limited to 12 months;[55] identify the data-transmitter institution or

FIGURE 8: Illustration of Consent Mechanism for Open Banking under the Brazil Framework



Source: Author's elaboration based on Banco Central do Brasil[57]

account service provider; specify the data or services that will be shared; and include the customer identification. If there is a change in purpose, validity period, data-transmitter institution, or account service provider, or if the data or service is to be shared, a new consent from the customer is required. It is expressly forbidden to obtain the customer's consent by means of a standard customer agreement, using a form with the agreement field filled out in advance, or on presumption, without the customer actively manifesting his or her will.[56] Overall the joint resolution is much more detailed and prescriptive than PSD2 in relation to requirements for consumer consent, but as discussed in the previous section on the data-protection framework, lawful data processing for credit does not require consumer consent.

PERSPECTIVE OF MEXICO

Mexican regulators approved Mexico's Law to Regulate Financial Technology Institutions (Fintech Law) in 2018. Article 76 established open banking in Mexico, to be further developed through secondary regulation. The Mexican law is broad in terms of scope of participants and data. Under article 76 of the Fintech Law, financial institutions, money transmitters, credit-reporting companies, clearing houses, financial technology institutions, and companies authorized to operate with novel models are required to establish APIs that enable connectivity and access to interfaces developed or managed by other regulated entities and third parties specialized in information technology, with the purpose of sharing open financial data, aggregate data, and transactional data.[58] The Fintech Law states that these entities are required to create APIs and must share the following three types of data:

- Open financials, which are nonconfidential data, including information on services offered and access points[59]
- Aggregate data, which is that related to the statistical information of its operations[60]
- Transactional data, which is that related to the use of financial products and services by a consumer

The authorities decided to start with the nonconfidential data and then move to transactional data and leave out of the scope the aggregate data. Of these categories, transactional data is relevant to open banking and to the issues discussed in this paper. Transactional data relates to the use of a product or service, including deposit accounts, credits, and access means contracted in the name of the customers of regulated entities, as well as information related to the transactions that customers have carried out or intend to carry out. This is personal data of the consumer. Under the Fintech Law, the transfer of data and information is subject to secondary regulation that governs the standards necessary for the interoperability of API, the requirements for regulated entities and third parties to obtain the authorization to access such data and information from the relevant authority, and the fees that regulated entities can charge for the transfer of data and

information. Technical and security standards have been published recently, but specific requirements for consent mechanisms have not been issued yet.[61]

Data protection for the private sector in Mexico is governed by the Federal Law[62] on the Protection of Personal Data Held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, PPD), which entered into force on July 6, 2010.[63] The PPD follows the European Union's data-protection model and includes similar definitions[64] and provisions regarding consent of the "data owner," the term used in the PPD to refer to the data subject,[65] and rights of data owners.[66] As in the European Union's model, processing is widely defined as the "collection, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data."[67] Interestingly, transfer is defined as "[a]ny data communication made to a person other than the data controller or data processor."[68] The PPD also has extraterritorial operation with some differences in comparison to the GDPR.[69]

The PPD requires that "data controllers must adhere to the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability under the Law."[70] Article 7 states that personal data must be collected and processed in a lawful manner in accordance with the provisions established by the PPD and other applicable regulations. Personal data must not be obtained through deceptive or fraudulent means. Article 8 requires that that "all processing of personal data will be subject to the consent of the data owner except as otherwise provided by this Law. Such consent will be explicit when communicated verbally, in writing, by electronic or optical means or via any other technology, or by unmistakable indications." The PPD distinguishes explicit consent from implied consent, which in article 8 of the DPP is called tacit consent: It will be understood that the data owner tacitly consents to the processing of his data when, once the privacy notice has been made available to him, he does not express objection. Article 17 provides that a privacy notice must be made available to data owners through print, digital, visual, or audio formats or any other technology when personal data is obtained from the data owner.[71] Where data has not been obtained directly from the data owner, the data controller must notify the data owner of the change in the privacy notice. Article 8 also states that consent may be revoked at any time without retroactive effects. For revocation of consent, the data controller, in the privacy notice, must establish the mechanisms and procedures for such action.

The PPD provides that financial or asset data[72] requires the explicit consent of the data owner, except as provided in articles 10 and 37. Article 10 (part IV) sets out the circumstances under which processing does not require consent and closely follows the European Union's model by providing that consent for the processing of personal data will not be necessary where "it has the purpose of fulfilling obligations under a legal relationship between the data owner and the data controller." The key difference from the GDPR is that, although the PPD does not specifically refer to the legitimate interest of the data controller, article 10 (part IV) is capable of applying to the legitimate interests of the controller. Article 37,[73] which enables domestic and international data transfers without consent, can similarly apply.[74]

The Fintech Law requires the supervisory commission and the central bank to establish technical standards for the interoperability of APIs, their governance, security, and consent mechanisms.[75] These standards are being issued progressively, and specific requirements for consent mechanisms have not been issued yet. However, considering the similarity of the PPD with the European Union's data-protection model, EU requirements for consent provide a reasonable starting point for expectations on future guidance from Mexican authorities. Mexico also has other legislation that covers data processing for specific purposes and consumer protection legislation, including legislation that applies specifically to users of financial services, so this will also require careful coordination. Overall, these laws may provide adequate consumer protection in the context of open banking. However, dispersing the relevant provisions across several pieces of legislation, rather than confining them within the open-banking law, can add complexity to understanding and applying relevant law.

CONSENT FOR OPEN BANKING IN INDIA

Open-banking regulation in India closely follows PSD2 and is focused on payments initially, following launch of the Unified Payment Interface.[76] Developed and managed by the National Payments Corporation of India, the Unified Payment Interface facilitates interbank transactions through an API framework built in part on Aadhaar. The second stage is data sharing by a new class of non-bank finance companies called account aggregators (AAs). Currently, the Non-Banking Financial Company-Account Aggregator (Reserve Bank) Directions, 2016, updated on November 22, 2019[77] (Master Direction), specifies a wide range of "financial information" that can be aggregated by an account aggregator.[78] This second stage of data

sharing is yet to be fully implemented, but the framework is in place.

Open banking in India will be subject to the nation's new Personal Data Protection Bill of 2019 (Indian DPA)[79] when it becomes law. On December 11, 2019, India's minister for electronics and information technology introduced an updated draft of the DPA in the Lok Sabha, India's lower house of parliament. The bill has been referred to a joint select committee which was due to report back to the Lok Sabha before the 2020 budget session of parliament, but this did not occur and timing for passage remains unclear.

The Indian DPA is modelled on the GDPR and follows its key provisions closely, including those discussed in this paper, although some different terminology is used. For example, whereas the GDPR refers to data subjects, they are called data principals in the Indian DPA.[80] Instead of data controllers, the Indian DPA refers to data fiduciaries. A data fiduciary is the entity that determines the purpose and means of the processing of personal data.[81] The Indian DPA has extraterritorial reach, as the GDPR has.[82]

Like PSD2, explicit consent is the stated basis of open banking in India. The Master Direction is more detailed than PSD2 in relation to the requirements for consent. Section 6 sets out the consent architecture.[83] Section 6.3 of the Master Direction provides that "the consent of the customer obtained by the AA shall be a standardized consent artefact which shall contain the following details, namely:

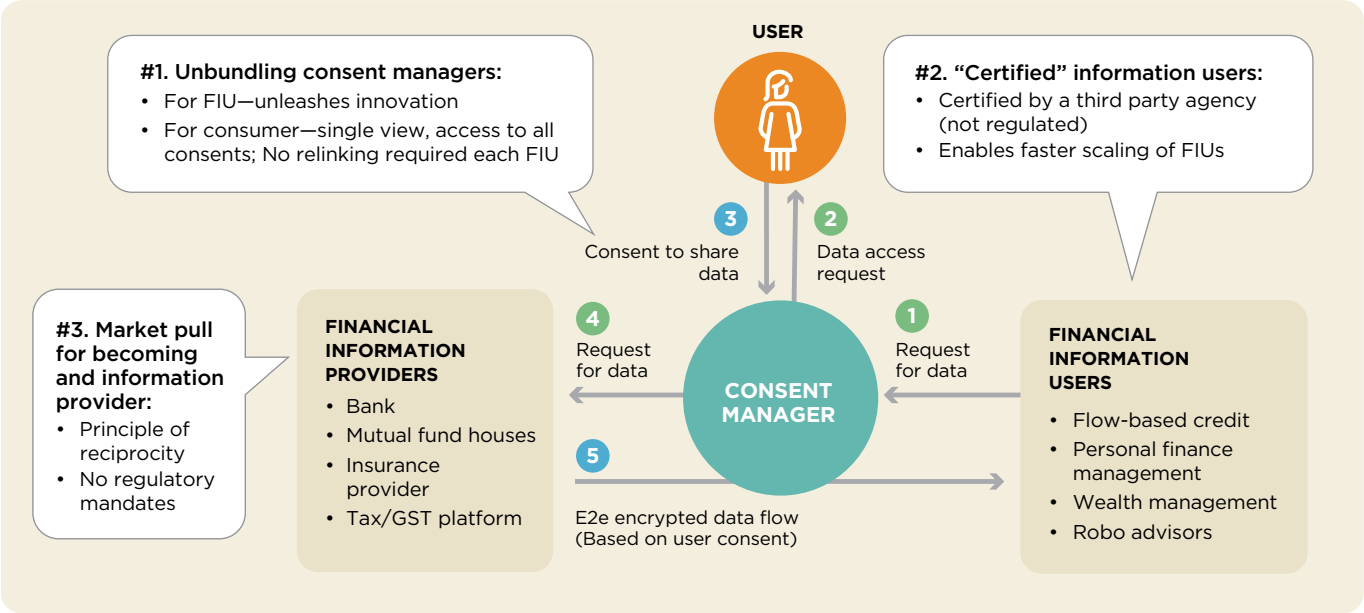
i. Identity of the customer and optional contact information;
ii. The nature of the financial information requested;
iii. Purpose of collecting such information;
iv. The identity of the recipients of the information, if any;
v. URL or other address to which notification needs to be sent every time the consent artefact is used to access information
vi. Consent creation date, expiry date, identity and signature/digital signature of the Account Aggregator; and
vii. Any other attribute as may be prescribed by the Bank."[84]

Under section 6.5, at the time of obtaining consent, the account aggregator shall inform the customer of all necessary attributes to be contained in the consent artefact and the right of the customer to file complaints with relevant authorities in case of non-redressal of grievances. An account aggregator "shall also provide its customers a functionality to revoke consent to obtain information that is rendered accessible by a consent artefact, including the ability to revoke consent to obtain parts of such information. Upon revocation, a fresh consent artefact shall be shared with the Financial Information provider."[85] Section 7 covers the sharing of financial information when a valid consent artefact is presented.[86] Section 10 sets out the rights of the customer, which include customer access to a record of the consents provided by him or her and the financial information users with whom the information has been shared.[87] A customer grievance policy is covered by section 11.[88]

The Indian DPA does not exactly mirror the sections of the GDPR that enable data processing without consent. Most significantly, the Indian DPA, like its Mexican equivalent, also does not contain the legitimate-interests ground that enables processing in the absence of consent. However, similar to the GDPR, the Indian DPA does allow processing without consent in the interests of prevention, detection, investigation, and prosecution of any offense or any other contravention of any law.[89] Clause 37 also states that "the Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law."[90]

Interestingly, the Indian DPA introduces the concept of a "consent manager," a data fiduciary that "enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform."[91] India enabled an intermediary that will be responsible for the customers' consent management. These intermediaries are licensed as non-banking financial companies. This is based on the concept of the account aggregator developed in India, which consolidates the financial information of a customer (called a financial institution user) held with different financial entities, spread across financial-sector regulators. Data cannot be stored in the aggregator and requires explicit consent and purpose specification. The difference in India with other jurisdictions is that other nonfinancial information can be retrieved and added with no consumer consent. To complement the consent framework, a set of core technical specifications have been framed by Reserve Bank Information Technology Private Ltd., a wholly owned subsidiary of the Reserve Bank of India, for adoption by all regulated entities, acting either as financial information providers or financial information users in November 2019. The key features of a consent mechanism in India include (i) the attributes to be contained in the consent

FIGURE 9: Illustration of Consent-Management Mechanism under Open-Banking Scheme



Source: Data Empowerment and Protection Architecture, National Institute for Transforming India, August 2020

format and the rights of the customer to file complaints, (ii) functionality to revoke consent, and (iii) the responsibility to verify—validity of the consent, specified date, and usage of it—and the credentials of the account aggregator rely on the financial information provider.

The Indian DPA also imposes additional requirements, such as a requirement to obtain the consent of a parent or guardian for the collection of a child's personal data.[92] Unlike the GDPR, the Indian DPA includes "financial data" in the definition of sensitive data, so that its processing requires explicit consent.

THE SITUATION IN RWANDA

On February 24, 2020, Rwanda gazetted Regulation 31/2019 of December 16, 2019 on Protection of Payment Service Users (Rwanda PSD), which closely follows the EU PSD2 in relation to payments. The Rwanda PSD is part of a suite of recent legislation governing payments.[93] The regulation sets out "the rules to protect the users of payment services provided totally or partially in Rwanda as well as the enforcement of rights and/or obligations in the provision of payment services."[94] The aim also appears to be to facilitate data sharing and encourage data portability as part of encouraging new market entrants, innovation, and competition, but at present the legislation covers payments. The regulation defines a payment-initiation service as "a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider."[95] The Rwanda PSD specifies that a payment service contract may be a single payment transaction contract[96] or a framework contract[97] and in transparency and required content of payment services contracts,[98] and also includes details on the information required before and after payment transactions.[99]

In 2020, Rwanda planned to enact a new Law on Data Protection and Privacy (Rwanda DPP). It was approved by the cabinet in October 2020 but has not been passed into law yet. The stated purpose of the DPP is "to provide mechanisms through which the protection and privacy of personal data will be ensured in connection with its processing in Rwanda; and to ensure the free flow of non-personal data within and outside Rwanda by laying down rules relating its protection."[100] Privacy is defined in the Rwandan DPP as "a fundamental right of a person to decide by whom, when, why, where, what and how his/her personal data can be accessed."[101] The Rwanda DPP follows the GDPR[102] very closely, including the principles of data protection, which the DPP extends to apply to "any involved third party,"[103] extraterritorial reach,[104] data subject rights, and other key provisions of the GDPR that relate to consent.

The Rwanda DPP requires that a person intending to act as a controller or processor must be registered as such.[105] Personal data is more simply defined as "any information relating to an identified or identifiable data subject,"[106] potentially casting a wider net than even the GDPR.

Consent of the data subject is defined in article 3(2) of the Rwandan DPP as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Like the GDPR, the Rwanda DPP gives the data subject the full right to withdraw his or her consent at any time and provides that its withdrawal does not affect the lawfulness of processing based on consent before withdrawal.[107]

The Rwandan law also includes additional details regarding valid consent. Article 7 covers the consent process, stating that "[T]he controller shall bear the burden of proof for establishing a data subject's consent to the collecting and/or processing of his/her personal data for a specified purpose. Consent is effective only when it is based on the data subject's free decision. The data subject shall be informed in advance of the consequence of his or her consent. The consent may be given in a form of a written statement including electronic means, or oral statement." The DPP also requires that "[T]he data subject's consent given in the context of a written declaration, which also contains other matters, shall be presented in a manner which is clearly distinguishable from those other matters, in an intelligible and easily accessible from using a clear, plain and understandable official language to the data subject. Any part of such a declaration which constitutes an infringement to the provision of this Law shall not be binding." Article 10 also clearly and succinctly covers consent of a child, stating that the "processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below that age, such processing shall be lawful only when it is given by either both parents or the legal guardian."

In article 43, the Rwanda DPP allows the processing of personal data in the absence of consent, including the legitimate-interests ground.[108] The Rwanda DPP does not specifically include explicit consent as a ground for lawful processing, and the grounds for processing in the absence of consent are generally broader. For example, article 11(a) permits processing that is "necessary for the purposes of carrying out the obligations of the data controller or data processor, or exercising specific rights of the data subject, in accordance with applicable Laws."[109]

Consent in Rwanda is also required when data is transferred across borders, with some exceptions. Under article 54 of the Rwanda DPP, a data controller or data processor may transfer or share personal data to another country where it has the authorization granted by the Rwanda data-protection authority and the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer, owing to the absence of appropriate safeguards. This article also allows transfer when "necessary" and, apparently, in the absence of consent of the data subject. The grounds listed as "necessary" are very similar to the non-consent grounds in article 43, including the legitimate-interest basis.

Customer consent is required under article 2 of the Rwanda PSD. The PSD regulation defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Article 22 covers consent and withdrawal of consent and provides the following:

"A payment service is considered to be authorized only if the payer has given consent to execute such a payment transaction or the execution of a series of payment transactions. Such consent

1 May be given before or, if agreed between the payer and its payment service provider, after the execution of the payment transaction;

2 Must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider;

3 May be given via the payee or a PISP."

The payer may withdraw its consent to a payment transaction at any time before the point at which the payment order can no longer be revoked, pursuant to article (5) of this regulation. Where consent does not exist for the execution of a payment transaction, then the payment transaction shall be deemed to be unauthorized. If consent for the execution of several payment transactions is revoked, then every subsequent payment transaction shall be deemed to be unauthorized. This approach mirrors that taken by PSD2 in the European Union as regards limits to withdraw consent.

Article 27, on automated decision-making and profiling, includes the right of a data subject not to be subject to a decision based solely on automated processing, including profiling, "which produces legal effects concerning him/her or significantly affects him/her." However, the DPP specifies significant exceptions, in addition to explicit consent,[110] including where the decision is "(a) necessary for entering into, or performing, a contract between the data subject and a controller and (b) authorized by a law or a regulation into force to which the controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests."

Interestingly, the law prohibits automated processing when it is based on sensitive data that is relevant to open banking in case financial data is used to develop credit scores. The legal provision concludes with this: "Any automated processing of personal data intended to evaluate certain personal aspects relating to an individual shall not be based on sensitive personal data." This is highly relevant to open banking because, as noted earlier, sensitive data is defined to include "property or financial details" and data revealing family details, "including names of the person's children, parents, spouse or spouses."

AUSTRALIA

In Australia, the term "open banking" is used as shorthand for the implementation of a new right in the banking sector, the Consumer Data Right (CDR). In essence, this "open banking" in Australia comprises three key elements: (i) customers having greater access to and control over their banking data; (ii) banks being required to share product and customer data with customers; and, (iii) with the consent of the customer, banks being required to share product and customer data with accredited third parties. The accreditation of third parties is addressed in rules produced by the Australian Competition and Consumer Commission (ACCC), the lead regulator for open banking.[111]

The Australian open-banking implementation is focused on data and not necessarily on customer account data. The banking and finance sector is the first sector to which the new right applies. The longer-term plan is for it to apply economy-wide. The CDR is enshrined in the Treasury Laws Amendment (Consumer Data Right) Act of 2019 (Cth), which inserts "Part IVD—Consumer data right" into the Competition and Consumer Act of 2010 (Cth) (CCA) that was passed on August 1, 2019,[112] to create the new CDR regime.[113] The framework established in Australia under the CCA includes rules[114] and standards governing how data is shared and detailed technical standards for sharing data.

The CDR gives consumers the right to share their data with the authorized third parties of their choice. Where an accredited person [115] is offering a good or service through the CDR regime and requires access to the consumer's CDR data to provide that good or service, the accredited person must obtain the consumer's consent to the collection and use of their CDR data. The regime is designed so that an accredited person can collect data only in response to a "valid request" from the consumer.[116] The consumer's consent to the collection and use of their CDR data is the basis of that request. The accredited person then collects this CDR data by making a "consumer data request"[117] to the relevant data holder or holders.

Three types of requests can be made to a data holder to disclose CDR data: (i) product data[118] requests made by any person; (ii) consumer data[119] requests made by eligible CDR consumers;[120] and (iii) consumer data requests made on behalf of CDR consumers by accredited persons. Consumer data is most relevant to the discussion in this paper. Consumer data relates to an identifiable, or reasonably identifiable, CDR consumer and is personal information.

The CDR is designed to be cross-sectoral and will eventually apply to a wider set of consumer data than banking data, which will initially be followed by energy data and telecommunications data, with the aim of enabling cross-sector data interoperability. "The Government expects that such data sharing will improve price transparency and facilitate comparison services that enable a customer to use price data, and data about their own spending and transactions, to choose products that are most appropriate for their personal or business circumstances, and facilitate switching from one provider to another" (Hamilton 2019).

As in other nations, there is more than one regulator, but the relationship and roles are more clearly defined with a dual-regulator model. The ACCC is lead regulator but is supported by the federal privacy regulator in Australia, the Office of the Australian Information Commissioner (OAIC). ACCC is responsible for assessing sectors for CDR application, accreditation criteria, overseeing the Data Standards Body, and strategic enforcement. The OAIC is responsible primarily for handling complaints from individuals and small and medium-sized enterprises. The OAIC is also responsible for advising the treasurer and the ACCC on the privacy implications of designating sectors.

Data protection in Australia is governed by the federal Privacy Act 1998 (Cth) (Privacy Act). It is based on a set of fundamental data-protection principles, the Australian Privacy Principles (APPs). However, the CDR Act includes privacy safeguards that apply specifically to CDR data.[121] The privacy safeguards in the CCA are comparable to the APPs in the Privacy Act and "seek to ensure the privacy and confidentiality of consumers' data by providing for only authorized access to, and use of, CDR data" (ACCC 2020, 14). The accreditation of persons collecting and using CDR data is subject to the privacy safeguards. Privacy Safeguard 3, for example, prohibits an accredited person from seeking to collect data under the CDR regime unless

it is in response to a "valid request" from the consumer. Privacy Safeguard 6 requires that the accredited person use or disclose a consumer's CDR data only in accordance with a current consent from the consumer.

The framework established in Australia under the CCA includes rules and standards governing how data is shared and detailed technical standards for sharing data. The Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules)[122] are based on the right to protection from unlawful or arbitrary interference with privacy under article 17 of the International Covenant on Civil and Political Rights.[123] The CDR Rules supplement the privacy safeguards in the CCA and include requirements for how consumer consent is obtained and used.

Consent in the CDR regime differs from consent under the Privacy Act in that the former requires the explicit consent of a consumer for the collection and use of CDR data by accredited persons. Consent must meet the requirements set out in the CDR Rules for the consent processes, including information that must be presented to consumers when they are being asked to give consent and how that information is to be presented. Without express consent, which can remain valid for a maximum period of only 12 months, the accredited person is not able to collect or use CDR data. As discussed in this paper, consent can be express or implied, and personal data can be lawfully processed in the absence of consent.[124] Under the Australian Privacy Act, an APPs entity, for example, can collect personal information other than sensitive information if the information is reasonably necessary for one or more of the entity's functions or activities.

The Australian government considers consent to be one of the key concepts underlying the CDR system. Consent must meet the requirements set out in the CDR Rules, and it underpins how an accredited person or accredited data recipient may collect and use CDR data in the CDR regime. Division 4.3 of the CDR Rules is designed to "ensure that consent given by a consumer to collect and use CDR data is voluntary; express; informed; specific as to purpose; time limited; and easily withdrawn."[125] In particular, the CDR Rules require that, in obtaining a valid request from a consumer, an accredited person must comply with prescribed requirements for asking for consent, including information to be presented to the consumer, restrictions on seeking consent and in providing information, and in relation to withdrawal and expiry of consent.[126]

An accredited person may collect and use CDR data only with the consent of the consumer and must ask for that consumer's consent in accordance with the consumer data rules (CDR Rules), which require that consent to be voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn and to comply with the data-minimization principle. The consent process must also comply with the CDR data standards and have regard to the Consumer Experience Guidelines, which set out best-practice interpretations of several CDR Rules relating to consent.[127] A data holder may disclose CDR data only with the authorization of the relevant CDR consumer or consumers.[128] Consumer consent is the basis for the information flow between a consumer, an accredited person, and the data holder.[129]

The CDR is designed to place the value and control of consumer data in the hands of the consumer. This is achieved by requiring the consumer's consent for the collection and use of their CDR data. Consumer consent for the collection and use of their data is the foundation of the CDR regime. Consent enables consumers to be the decision-makers in the CDR regime, ensuring that they can direct where their data goes in order to obtain the most value from it.[130] The rules are intended to ensure that requests for consent to collect and use CDR data are transparent and that consumers understand the potential consequences of what they are consenting to,[131] and the rules achieve that objective. In addition to covering the essential elements, the rules include additional practical guidance, including specific examples that are supplemented with additional, coordinated guidance from the OAIC that includes key concepts in bullet-point format and additional examples of compliant and noncompliant consent practices.[132] CDR prohibits an accredited person from requesting consent from consumers to use, or from disclosing their data for the purpose of selling it, unless such data can no longer be traced back to the consumer. 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. The Australian approach coordinates with the general data-protection legislation but includes specific requirements for consumer consent and data protection for open-banking data in the open-banking regulation, creating more clarity and certainty on what is required than in countries where the separate requirements of open-banking legislation and data-protection laws must be reconciled.

NOTES

41. See Banco Central do Brasil, Regulation on Open Banking, Joint Resolution No. 1 of May 4, 2020, and Circular No. 4.015 of May 4, 2020, which create the rules for the functioning of open banking in Brazil.
42. https://www.bcb.gov.br/detalhenoticia/17261/nota
43. Article 5 sets out the minimum required data sharing. It includes data on (a) service channels that relates to the institution's offices and branches; domestic correspondents; electronic channels; and other channels available to customers. It also includes data on (b) products and services related to deposit accounts; savings accounts; prepaid payment accounts; post-paid payment accounts (credit cards); credit operations; foreign exchange operations; acquiring services in payment schemes; term deposit accounts and other investment products; insurance; and open pension funds. It also requires sharing of data on (c) registration of customers and their representatives and (d) customer transactions related to deposit accounts; savings accounts; prepaid payment accounts; post-paid payment accounts (credit cards); credit operations; payroll accounts, as disciplined by Resolution No. 3,402, dated September 6, 2006; foreign exchange operations; acquiring services in payment schemes; term deposit account and other investment products; insurance; and open pension funds; and services for initiating payment transactions; and forwarding loan proposals. Consent must be obtained from the customer, pursuant to article 10, for purposes of sharing registration and transactional data and services referred to in subitems "c" and "d," and in the case of data and services related to the customer.
44. See section VI of the joint resolution.
45. Article 3 of the joint resolution.
46. Article 4 of the joint resolution.
47. Article 40 requires the institutions to establish monitoring and control mechanisms to ensure the reliability, availability, integrity, security, and confidentiality that are the subject of articles 31 and 39, as well as the implementation and effectiveness of the requirements that are the subject of this joint resolution, including auditing processes, tests, and audit trails; metrics and compatible indicators; and identification and correction of eventual deficiencies. This process includes records of consent, authentication, confirmation, and consent revocation of the sharing, information concerning the shared data and services, including customer identification credentials; notifications received regarding the subcontracting that is the subject of article 38, item VI, adoption of security measures for receiving and archiving by the partner of the data or information about shared services when it applies; and communications received about incidents that are the subject of article 38, section 3, if any have occurred. Monitoring and control mechanisms are subject to periodic testing by internal auditing personnel, when applicable, compatible with the institution's internal controls; compatible with the institution's cybersecurity policy, as foreseen by the current regulation; and ensure that the other institutions involved in the sharing do not have access to the credentials used by the customer for identification and authentication purposes.

    Article 41. The institution's monitoring and control mechanisms shall encompass indicators pertaining to the performance of the interfaces used for the sharing. The convention that is the subject of article 44 may define additional indicators related to the performance of the interfaces as well as mechanisms of transparency and disclosure of such indicators to the general public.
48. *Customer* is used in the joint resolution instead of consumer. The scope of open banking is broader in Brazil than in PSD 2 in that *customer* is defined in article 2, part II, of the joint resolution to include legal entities as well as natural persons. When discussing the Brazilian scheme, *customer* is used instead of *consumer* for consistency, but the focus in this paper remains on implications for individuals.
49. Article 5, section 3, of the joint resolution.
50. Article 5, section 4, parts I and II.
51. Article 5, section 5, parts I and II of the joint resolution.
52. The LGPD was passed by the National Congress of Brazil on August 14, 2018, and came into effect on September 18, 2020. Prior to the LGPD, personal data-protection in Brazil was covered by many legal norms at the federal level, the Civil Rights Framework for the Internet (Internet Act), and the Consumer Protection Code. The LGPD provides more clarity.
53. Article 7, part X, of the LGPD.
54. Article 10, section 4, requires that information not be shared with the data-transmitter institution about the purpose but as set out in article 10, section 5. This does not apply to partnership agreements under article 36 or in other cases permitted by the framework.
55. In the case of successive payment transactions, the customer, at his/her discretion, may determine a longer validity period under article 10, section 6.
56. Article 10, section 3, of the joint resolution.
57. Based on a presentation about open banking by Diogo Silva, Banco Central do Brasil, February 2021.
58. The general dispositions issued by the National Banking and Security Commission (*Comisión Nacional de Banca y Valores, CNBV*) and Banco de México establish the common technical standards to ensure the interoperability of APIs. The Fintech Law also requires the development of secondary regulations by the CNBV for banks and financial institutions, including the new financial technology institutions, and by Banco de México for payment systems, central counterparties, and credit-reporting systems. The secondary regulations also establish the security mechanisms to access, send, and obtain data and information and outline the information considered critical to the APIs.
59. Open financial data does not contain confidential information, such as information on products and services offered to the general public by the regulated entities, the location of their offices and branches, ATMs, or other access points to their products and service.

60. Aggregate data is statistical information related to transactions performed by or through regulated entities but not disaggregated in a manner that could identify customer's personal data or transactions
61. On June 4, 2020, the CNBV published in the official federal gazette the regulations governing the APIs referred to in the Fintech Law (API Regulations). Financial institutions, money transmitters, financial technology institutions, and companies authorized by the CNBV are subject to the API Regulations that apply to the transfer of data and information that can be shared through the API. The API Regulations govern the transfer and access of only open data. On March 10, 2020, the Mexican central bank published in the gazette Rule 2/2020 applicable to credit-reporting companies and clearing houses, as required under article 76 of the Fintech Law regarding standardized APIs.
62. The executive branch has also issued the Regulations to the Federal Law on the Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, or the Regulations*), which entered into force on December 22, 2011; the Privacy Notice Guidelines (the Guidelines), which entered into force on April 18, 2013; the Recommendations on Personal Data Security, issued on November 30, 2013; the Parameters for Self-Regulation regarding personal data, which entered into force on May 30, 2014; and the General Law for the Protection of Personal Data in Possession of Obligated Subjects (*Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*), which entered into force on January 27, 2017.
63. The most relevant pieces of legislation addressing personal data protection in Mexico are the Constitution; the Private Data Protection Law; the Governmental Data Protection Law; the Regulations of the Private Data Protection Law; the Guidelines for Privacy Notices; and the Self-Regulation Parameters on Data Protection, which are applicable to the private sector. On September 28, 2018, the official federal gazette published the decree issuing the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981 (Convention 108) and its additional protocol dated November 8, 2001 (ETS 181). Also, on March 21 and 22, 2019, the Ministry of Finance and Public Credit issued several provisions that amend, add, and eliminate different articles of the General Provisions for the Prevention of Money Laundering and Terrorism Financing applicable to the services that may be rendered by financial entities, such as credit institutions and exchange offices. These are services such as opening accounts, entering into agreements. or performing financial operations through the use of the internet or mobile devices. Financial entities will request geolocalization of clients, as well as biometric data, such as voice and image matching, to perform such operations and will, therefore, require express written consent from clients. In May 2019, the National Institute of Transparency, Access to Information and Protection of Personal Data also published nonbinding guidelines in relation to different tools and applications that may be used by parents to supervise or limit access and content in mobile devices used by their children. This is to protect children from disclosing their personal data on unsecured sites. See César G. Cruz Ayala and Marcela Flores González, "The Privacy, Data Protection and Cybersecurity Law Review: Mexico," The Law Reviews, November 5, 2021, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210064/mexico.
64. Article 3 of the Mexican PPD defines consent as "[E]xpression of the will of the data owner by which data processing is enabled." Personal data is "[A]ny information concerning an identified or identifiable individual," and sensitive personal data is "[P]ersonal data touching on the most private areas of the data owner's life, or whose misuse might lead to discrimination or involve a serious risk for said data owner. In particular, sensitive data is considered that which may reveal items such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views, sexual preference." Like the GDPR, financial information is not specifically included in this definition. Like the GDPR, consent to processing of sensitive data must be express. Article 9 of the Mexican PPD states that "in the case of sensitive personal data, the data controller must obtain express written consent from the data owner for processing, through said data owner's signature, electronic signature, or any authentication mechanism established for such a purpose. Databases containing sensitive personal data may not be created without justification of their creation for purposes that are legitimate, concrete and consistent with the explicit objectives or activities pursued by the regulated party." Data processor is "[T]he individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller," and the data processor is "[T]he individual or legal entity that, alone or jointly with others, processes personal data on behalf of the data controller." See parts IV, V, VI, IX, and XIV of article 3, Mexican PPD.
65. Article 3, part XVII, defines data owner as the "individual to whom personal data relates."
66. Chapter III, Mexican PPD.
67. Article 3, part XVIII, Mexican PPD.
68. Article 3, part XIX, Mexican PPD.
69. The Mexican PPD applies to data processors not located in Mexico that process personal data on behalf of data controllers located in Mexico; data controllers that are not located in Mexico, but that are subject to Mexican laws as a result of an agreement or in terms of international laws; and data controllers using a processing means located in Mexico (even if they are not established in Mexico), except if those means are merely for transit purposes, without involving the processing of personal data. César G. Cruz Ayala and Marcela Flores González, "The Privacy, Data Protection and Cybersecurity Law Review: Mexico," The Law Reviews, November 5, 2021, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210064/mexico.
70. Article 6, Mexican PPD.

71. Article 17 states that "the privacy notice must be made available to data owners through print, digital, visual or audio formats or any other technology, as follows:
    I. Where personal data has been obtained personally from the data owner, the privacy notice must be provided at the time the data is collected, clearly and unequivocally, through the format by which collection is carried out, unless the notice has been provided prior;
    II. Where personal data are obtained directly from the data owner by any electronic, optical, audio or visual means, or through any other technology, the data controller must immediately provide the data owner with at least the information referred to in sections I and II of the preceding article, as well as provide the mechanisms for the data owner to obtain the full text of the privacy notice.

    Where data has not been obtained directly from the data owner, the data controller must notify him of the change in the privacy notice." Article 17 contains the following proviso: "Where it is impossible to provide the privacy notice to the data owner or where disproportionate effort is involved considering the number of data owners, or the age of the data, with the authorization of the Institute, the data controller may implement compensatory measures."
72. "Financial or asset data" is not defined in the Mexican PPD.
73. Article 37 states that domestic or international transfers of data may be carried out without the consent of the data owner in the following cases:
    "I. Where the transfer is pursuant to a Law or Treaty to which Mexico is party;
    II. Where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management;
    III. Where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies;
    IV. Where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party;
    V. Where the transfer is necessary or legally required to safeguard public interest or for the administration of justice;
    VI. Where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and
    VII. Where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data owner."
74. See parts IV and also III, article 37, Mexican PPD. The Mexican PPD generally follows the GDPR in relation to individual rights, but there is a single article that contains overall limitations. Article 4 provides that "[T]he principles and rights under this Law will have, as a limit with regard to their observance and exercise, protection of national security, public order, health and safety as well as the rights of third parties." A third party is defined in, part XVI of article 3 as a "Mexican or foreign individual or legal entity other than the data owner or data controller," which in application can be less limiting to the rights of the data owner than the GDPR. However, this is tempered by articles 10 and 37.
75. On June 4, 2020, the Mexican Banking and Securities Commission published in the official federal gazette the Regulations Governing the Applications Programming Interfaces Referred to in the Fintech Law (API Regulations). Financial institutions, money transmitters, financial technology institutions, and companies authorized by the CNBV are subject to the API Regulations, which apply to the transfer of data and information that can be shared through the API. The API Regulations govern the transfer and access of only open data, not transactional data. Similarly, on March 10, 2020, the Mexican central bank published in the gazette Rule 2/2020 applicable to credit-reporting companies and clearing houses, as required under article 76 of the Fintech Law regarding standardized application programming interfaces (Rule 2/2020). Rule 2/2020 does not govern the requirements for the transfer and access of transactional data and provides only that, upon the respective clearing house or credit-reporting company obtaining its authorization to create an API for aggregate data and open data (as applicable), it must submit an additional application for the authorization to transfer transactional data, in accordance with the requirements set forth by the Mexican central bank through secondary regulation. The Fourth Transitory Article of Rule 2/2020 provides that, prior to the submission of the referred application, the entity must submit, no later than March 5, 2021, its proposal of the type of data and information that must be included in this category, as well as the mechanisms for the authentication, identification, and obtaining of data, in addition to the express consent of the respective customers. Rule 2/2020 will become effective on March 5, 2021. Clearing houses and credit-reporting companies will have a period of 360 days from the date of effectiveness of Rule 2/2020 to obtain the authorization from the Mexican central bank to create APIs for open data and aggregate data.
76. The Unified Payment Interface is an instant real-time payment system that allows users to perform interbank money transfers and pay retail merchants directly from a bank account through mobile applications such as Google Pay, PhonePe, Paytm, and BHIM.
77. RBI/DNBR/2016-17/46. Master Direction DNBR.PD.009/03.10.119/2016-17.
78. See section 3(xi), Master Direction,
79. Bill No. 373 of 2019. The Indian DPA and the report *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf) resulted from the landmark case of *K.S. Puttaswamy v. Union of India* (2017), in which the Full Court of the Supreme Court of India affirmed the right to privacy as a fundamental right. The bill's preamble reflects this: "[T]he right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy"; "[T]he growth of the digital economy has expanded the use of data as a critical means of communication between persons"; and "[I]t is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation through digital governance and inclusion."

80. Clause 3 (14), Indian DPA.
81. Clause 3 (13), Indian DPA. There are also local storage requirements. "Critical personal data" must be stored and processed only in India. "Critical personal data" is defined to mean "such personal data as may be notified by the Central Government to be the critical personal data." See clause 33, DPA. "Sensitive personal information" must also be stored within India's geographical borders but can be copied elsewhere provided certain conditions are met. This includes a provision that closely follows the GDPR's adequacy requirement—that is, for data to be copied into another country, the destination country must have sufficient privacy protections and not impede Indian law enforcement access to the data. The local storage requirement is in line with the requirement of the Reserve Bank of India for local storage of payment data.
82. Clause 2, Indian DPA.
83. Section 6 provides that:

    "6.1 No financial information of the customer shall be retrieved, shared or transferred by the Account Aggregator without the explicit consent of the customer.

    6.2 An Account Aggregator shall perform the function of obtaining, submitting and managing the customer's consent in accordance with these directions."
84. Section 6.4 states that the consent artefact can also be obtained in electronic form. Section 6.7 adds that an electronic consent artefact shall be capable of being logged, audited, and verified.
85. Section 6.6.
86. "7.1 Financial Information providers shall share financial information of a customer with an Account Aggregator on being presented a valid consent artefact by an Account Aggregator in accordance with Clause 6.

    7.2 Upon being presented the consent artefact, the Financial Information provider shall verify:

    (a) validity of consent

    (b) specified dates and usage; and

    (c) the credentials of the Account Aggregator

    through appropriate means.

    7.3 Upon due verification, the Financial Information providers shall digitally sign the financial information and securely transmit the same to the Account Aggregator in accordance with the terms contained in the consent artefact.

    7.4 All responses of the Financial Information provider shall be in real time.

    7.5 To enable these data flows, the Financial Information providers shall:

    a. implement interfaces that will allow an Account Aggregator to submit consent artefacts, and authenticate each other, and would enable secure flow of financial information to the Account Aggregator;

    b. adopt means to verify the consent including digital signatures, if any, contained in the consent artefact;

    c. implement means to digitally sign the financial information that is shared by them about the customers;

    d. maintain a log of all information sharing requests and the actions performed by them pursuant to such requests, and submit the same to the Account Aggregator.

    7.6 Use of information by Account Aggregator and Financial Information user

    7.6.1 Where financial information has been provided by a Financial Information provider to an Account Aggregator for transferring to a Financial Information user with the customer's explicit consent, the Account Aggregator shall:

    i. verify the identity of the Financial Information user; and, if verified,

    ii. securely transfer the customer's information to the intended recipient in accordance with the terms of the consent artefact.

    7.6.2 Where financial information has been provided by a Financial Information provider to an Account Aggregator for transferring to the customer or to a Financial Information user, it shall not be used or disclosed by an Account Aggregator or the Financial Information user except as may be specified in the consent artefact."
87. "10. Rights of the customer

    a) An Account Aggregator shall enable the customer to access a record of the consents provided by him and the Financial Information users with whom the information has been shared.

    b) An Account Aggregator shall not use or access any customer information other than for performing the business of account aggregator explicitly requested by the customer.
88. "11. Customer Grievance

    11.1 An account aggregator shall have in place a Board approved policy for handling/disposal of customer grievances/complaints. It shall have a dedicated set-up to address customer grievances/complaints.

    11.2 Customer complaints shall be handled/disposed of by the Account Aggregator within such time and in such manner as provided for in its Board approved policy, but in any case, not beyond a period of one month from its receipt.

    11.3 At the operational level, Account Aggregator shall display the following information prominently, for the benefit of customers, on the website and at the place/s of business:

    (a) the name and contact details (Telephone/Mobile nos. as also email address) of the Grievance Redressal Officer who can be approached by the public for resolution of complaints against the company.

    (b) that if the complaint/dispute is not redressed within a period of one month, the customer may appeal to the Bank."

89. Clause 36 specifies that the consent requirements do not apply where: "(a) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force; (b) disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding."
90. There are also local storage requirements. "Critical personal data" must be stored and processed only in India. "Critical personal data" is defined to mean "such personal data as may be notified by the Central Government to be the critical personal data." See clause 33, DPA. "Sensitive personal information" must also be stored within India's geographical borders but can be copied elsewhere provided certain conditions are met. This includes a provision that closely follows the GDPR's adequacy requirement—that is, for data to be copied into another country, the destination country must have sufficient privacy protections and not impede Indian law enforcement access to the data. See clauses 33 and 34, Indian DPA. The local storage requirement is in line with the requirement of the Reserve Bank of India for local storage of payment data. See clauses 33 and 34, Indian DPA.
91. See clause 21 and clause 23(3), (4), and (5).
92. Clause 16, Indian DPA.
93. See National Bank of Rwanda, Laws and Regulations, https://www.bnr.rw/laws-and-regulations/payment-system/laws-regulations.
94. Article 1, Rwanda PSD.
95. Article 2, Rwanda PSD.
96. Defined in article 2 as "a contract for a single payment transaction not covered by a framework contract."
97. Defined in article 2 as "a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account to execute such transaction."
98. Chapter III, Rwanda PSD.
99. Articles 17–20, Rwanda PSD.
100. Article 1, Rwanda DPP.
101. Article 2(17), Rwanda DPP. The right to privacy is enshrined in article 22 of the Constitution of Rwanda as follows: "The private life, family, home or correspondence of a person shall not be subjected to arbitrary interference; his or her honour and good reputation shall be respected. A person's home is inviolable. No search of or entry into a home may be carried out without the consent of the owner, except in circumstances and in accordance with procedures determined by law. Confidentiality of correspondence and communication shall not be subject to waiver except in circumstances and in accordance with procedures determined by law." This article is clearly adopted from similar articles in international treaties, including those that are the foundation for the GDPR.
102. There are some significant differences, though, including the inclusion of several new concepts. These include "confidential data," which is defined in article 2(3) as "data that might be less restrictive within the entity but might cause damage if disclosed." Confidential data is classified as nonpersonal data pursuant to article 4. The DPP also introduces the concept of "data embassies," which are defined as "a physical or virtual data center in an allied foreign country that stores data of critical government information systems and mirrors critical service applications." See article 2(7) and chapter VII regarding data sharing, transfer storage, and retention.
103. See article 5, Rwanda DPP.
104. See article 2, which states: "This law shall apply to any person who processes data whether:
    i. Done by electronic or other means using data through an automated or non-automated platform, forming or intending to form part of a filing system;
    ii. Established or ordinarily resident in Rwanda that processes data while in Rwanda; or
    iii. Not established or not ordinarily resident in Rwanda, but processing personal data of data subjects located in Rwanda.
    iv. Non-personal data is provided as a service to users residing or having an establishment in Rwanda."
105. See article 30, which states that "[A]ny person who intends to act as controller or processor shall first register with the authority in charge of personal data protection and privacy. The Authority in charge of data protection and privacy shall prescribe thresholds required for mandatory registration by considering the nature of industry, volumes of data processed, whether it is a sensitive personal data and any other criteria as the Authority in charge of data protection and privacy under this article may specify." See also article 31 for the information that must be supplied to register: "Every application under paragraph (1) shall be accompanied by the following particulars regarding the applicant:
    (a) name and address;
    (b) if he/she or it has nominated a representative for the purposes of this Law, the name and address of the representative;
    (c) a description of the personal data to be processed by the controller or processor, and of the category of data subjects, to which the personal data relate;
    (d) a statement as to whether or not he/she or it holds, or is likely to hold, special categories of personal data;
    (e) a description of the purpose for which the personal data are to be processed;
    (f) a description of any recipient to whom the controller intends or may wish to disclose the personal data;
    (g) the name, or a description of, any country to which the proposed controller intends or may wish, directly or indirectly, to transfer the data;
    (h) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of the personal data; and
    (i) Any other requirement as may be determined by the authority in charge of data protection and privacy." Chapter V specifies the obligations and duties of controllers and processors, and generally follows the GDPR.

106. Article 3 (14), Rwanda DPP.
107. Article 9, Rwanda DPP. The data subject must be informed of this right prior to giving consent, and "withdrawal shall be as easy as giving consent." See article 9, Rwanda DPP.
108. Article 43, entitled "Lawful processing," the equivalent of article 6(1) of the GDPR, states that:

    "Personal data shall be processed only when:

    (a) the data subject consents to the processing for one or more specified purposes;

    (b) the processing is necessary:

    (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

    (ii) for compliance with any legal obligation to which the controller is subject;

    (iii) in order to protect the vital interests of the data subject or another person;

    (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

    (v) the performance of any task carried out by a public entity;

    (vi) the exercise, by any person in the public interest, of any other functions of a public nature;

    (vii) for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or

    (viii) for the purpose of historical, statistical or scientific research upon authorization by relevant institution." (Emphasis added.)
109. Article 12 specifies required safeguards when sensitive information is processed.
110. The wording used in article 27 is "based on the data subject's explicit consent" (emphasis added), which opens the range of possibilities as to exactly how this can apply in practice.
111. These rules are the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) pursuant to section 56B, CCA.
112. CCA, https://www.legislation.gov.au/Details/C2019A00063/Html/Text.
113. The "CDR regime" was enacted by the Treasury Laws Amendment (Consumer Data Right) Act 2019 to insert a new part IVD into the CCA. The CDR regime includes the CDR Rules, privacy safeguards, data standards, designation instruments, and any regulations made in respect of the provisions in the CCA. See OAIC, "Chapter B: Key Concepts," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-b-key-concepts/#ftn12.
114. These rules are the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) pursuant to section 56B, CCA.
115. Under section 56CA(1), an "accredited person" is a person who has been granted accreditation by the Data Recipient Accreditor of the ACCC, in accordance with part 5 of the CDR Rules. There is some change in terminology depending on whether data has been collected. For example, where an accredited person seeks consent from a consumer to collect and use CDR data, and subsequently seeks to collect that data, they do so as an accredited person because they are yet to collect the data. When an accredited person has disclosed CDR data, under the CDR Rules they are both an accredited data recipient and an accredited person. See OAIC, "Chapter B: Key Concepts," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy safeguard-guidelines/chapter-b-key-concepts/#ftn12.
116. Rule 4.3 (3), CDR Rules.
117. Rule 4.3 (5), CDR Rules.
118. Product data is data for which there are no CDR consumers. Product data requests can be made in respect of required product data and voluntary product data. Required product data include eligibility criteria, terms and conditions, price, availability or performance of a product (if publicly available), and product-specific data.
119. Consumer data requests can be made in respect of required consumer data and voluntary consumer data. Required consumer data includes customer data identifying or about a particular person; account data about the operation of an account; transaction data identifying or describing a transaction; and product-specific data in relation to a particular product that a particular person uses. Consumer data is most relevant to the discussion in this paper.
120. "CDR consumer" is defined in section 56AI(3), CCA: A person is a CDR consumer for CDR data if (a) the CDR data relates to the person because (i) of the supply of a good or service to the person or to one or more of the person's associates (within the meaning of section 318 of the Income Tax Assessment Act of 1936) or (ii) of circumstances of a kind prescribed by the regulations; and (b) the CDR data is held by another person who (i) is a data holder of the CDR data, (ii) is an accredited data recipient of the CDR data, or (iii) is holding the CDR data on behalf of a person mentioned in subparagraph (i) or (ii); and (c) the person is identifiable, or reasonably identifiable, from (i) the CDR data or (ii) other information held by the other person referred to in paragraph (b); and (d) none of the conditions (if any) prescribed by the regulations apply to the first-mentioned person in relation to the CDR data. Only "eligible" CDR consumers are able to make consumer data requests under the rules. Schedule 3, clause 2.1, provides, among other things, that a CDR consumer for the banking sector is eligible "if the consumer: a. is 18 years or older (if the person is an individual as opposed to a business); and b. has at least one account with the data holder (receiving the request) that is an open account and set up in such a way that it can be accessed online." See ACCC (2020), 14.
121. See also Competition and Consumer (Consumer Data Right) Rules 2020, https://www.legislation.gov.au/Details/F2020C00554.
122. CDR Rules, https://www.legislation.gov.au/Details/F2020C00554.

123. "The rules invoke the right to protection from unlawful or arbitrary interference with privacy under Article 17 of the International Covenant on Civil and Political Rights because they enable consumers to authorise data sharing and use in a regulated manner that is subject to the Privacy Safeguards. The rules provide individuals and businesses with a right to access data relating to them, and to consent to secure access to their data by accredited third parties." The rules are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011. See ACCC (2020), 12.
124. Depending on whether the data is "sensitive" as defined in the section 6(1) of the Privacy Act and the circumstances requiring its processing. The act does not specifically include the legitimate-interests ground like the GDPR but sets out general situations where processing without consent is lawful. Permitted general situations include the following:
    - When it is unreasonable or impracticable to obtain the individual's consent to the collection, use, or disclosure
    - The entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities, has been, is being or may be engaged in
    - The entity reasonably believes that the collection, use, or disclosure is reasonably necessary to assist an entity, body, or person to locate a person who has been reported as missing
    - The collection, use, or disclosure is reasonably necessary for the purposes of a confidential alternative dispute-resolution process

    See section 16A, Privacy Act. Health situations are set out in section 16B.
125. See ACCC (2020), 94.
126. Rules 4.10–4.14, CDR Rules.
127. See rule 4.10, CDR Rules. The guidelines are also discussed in OAIC, "Chapter B: Key Concepts," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-b-key-concepts/#ftn12.
128. See OAIC, "Chapter B: Key Concepts," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-b-key-concepts/#ftn12.
129. See OAIC, "Chapter C: Consent—The Basis for Collecting and Using CDR Data," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-c-consent-the-basis-for-collecting-and-using-cdr-data/.
130. See OAIC, "Chapter C: Consent—The Basis for Collecting and Using CDR Data," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-c-consent-the-basis-for-collecting-and-using-cdr-data/.
131. See ACCC (2020), 93–114.
132. OAIC, "Chapter C: Consent—The Basis for Collecting and Using CDR Data," February 24, 2020, https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-c-consent-the-basis-for-collecting-and-using-cdr-data/.

6

CONCLUSIONS AND EMERGING GOOD PRACTICES

The combination of rigorous consent and other complementary approaches can provide greater control for consumers and help reduce the likelihood that they may be harmed by innovations such as open banking through the sharing of their personal data. Table 1 provides further information on policies and interventions discussed in this paper that can be used together to strengthen consumer data protection and privacy. While each of the policies and interventions has pros and cons, in combination they can improve consumers' data security and privacy.

Questions such as which policies work in which regulatory environments, which is more effective in different populations with varying levels of literacy and connectivity, and what the costs are—to consumers, providers, and regulators—of different approaches are all areas where further research is needed.

All open-banking schemes that involve access to customer account data require consumer consent to access data, as open banking is based on access to permissioned account data. This is also a means of enabling data portability and allowing consumers to make use of their information to acquire additional services that may be more convenient or even less costly from a broader range of service providers.

Although consent forms in the past were considered lengthy and difficult to read and understand by consumers, technology can enable the design of consent mechanisms that allow consumers broader control over their data than was permitted by paper forms or boxes ticked on a website. The consent platforms that are currently being designed allow consumers to keep track of the consents they provide, to make a one-time choice or choose throughout the provision of the service, to choose the type of accounts that are accessed, and to withdraw consent within some limits.

The approach taken by the CDR in Australia aims at increasing the control of consumers over their own data while also including additional safeguards to the data-flow process through an accreditation process. This approach is similar to the one taken in the United Kingdom, which restricts participation in the open banking to a limited number of institutions, all of which are under the regulatory perimeter of the financial authority and subject to data-protection safeguards.

TABLE 1: Strengthening Consumer Data Protection and Privacy in Open Banking

POLICY / INTERVENTION	KEY ELEMENTS	PROS	CONS
Legal framework for consumer data protection and privacy in open banking	Data protection and privacy addressed clearly in open-banking law	Necessary foundation for regulation, supervision, enforcement, litigation	Necessary but not sufficient—first of many steps for effective consumer data protection and privacy[134]
Strengthening consent—explicit consent elements: – Freely given – Unambiguous – Informed – Time bound – Specific purpose – Ability to withdraw – Clear language	No preticked boxes or implied consent from scrolling on a website; consent separate from other contract terms; withdrawal as easy as providing consent	Customers involved in decision on data sharing; provides opportunity to inform and educate consumers on data-protection issues when consent is solicited	Consumer control may be illusory if consent is required to obtain financial services; may not be effective in practical terms if consumers don't read or can't understand consent
Platforms for consumers to follow their data and where they have provided consent	Accessible, easy to navigate, potential for alerts	Increases transparency on use of data; enables consumers to identify misuse	Consumers who are most vulnerable may be less likely to use these tools; uneven access to technology creates gaps in protection
Legitimate purpose	Focused in areas where benefits to consumers are clear; allowance for use of anonymized data for innovation	Provides clarity for both providers and consumers on use cases	May result in less innovation if purposes are narrowly defined; relies on providers following rules, so may not work in a weak institutional environment
Notification of adverse action	Timely communication to consumers via preferred channels; mechanism for resolution/rectification	Focuses attention on instances of harm, so effort is expended by consumers where most needed	Reactive policy, so problems not detected until harm has been caused (such as denial of credit)
Regulatory oversight	Leverage technology (regtech, suptech); utilize investigative tools (for example, mystery shopping); ability to levy penalties, legal action	Regulators have greater skills and resources than consumers to hold providers accountable; can intervene to stop systematic abuses	Regulators may lack resources for effective oversight; regulators may be slow to recognize new abuses, providing limited relief to consumers
Privacy by design	Data minimalization; use of secure technologies (encryption, multifactor authentication); avoiding unnecessary data archives	Reduces risk of misuse of personal data starting with the product design and functionality; may reduce risks to consumers and need for regulation if done well	May give a false sense of security; technology may evolve in ways that reduces privacy protections over time
Privacy by design	Data minimalization; use of secure technologies (encryption, multifactor authentication); avoiding unnecessary data archives	Reduces risk of misuse of personal data starting with the product design and functionality; may reduce risks to consumers and need for regulation if done well	May give a false sense of security; technology may evolve in ways that reduces privacy protections over time

NOTE

134. Other critical elements, once the legal framework is in place, include a strong regulatory framework, resources for adequate oversight and supervision by regulators, consumer awareness of their rights in law and regulation, industry standards to maintain secure and appropriate use of personal data, and mechanisms to facilitate consumer access to relevant information on data use.

REFERENCES

ACCC (Australian Competition and Consumer Commission). 2020. *Explanatory Statement: Competition and Consumer (Consumer Data Right) Rules 2020,* https://www.legislation.gov.au/Details/F2020L00094/Explanatory%20Statement/Text.

Barron, John M., and Michael E. Staten. 2003. "The Value of Comprehensive Credit Reports: Lessons from the US Experience." In Miller, Margaret, *Credit Reporting Systems and the International Economy,* edited by Margaret J. Miller, 273–310. MIT Press, Cambridge, Massachusetts.

BCBS (Basel Committee on Banking Supervision). 2019. *Report on Open Banking and Application Programming Interfaces.* Bank for International Settlements, Basel, Switzerland.

Berg, Gunhild, and Bilal Zia. 2017. "Harnessing Emotional Connections to Improve Financial Decisions: Evaluating the Impact of Financial Education in Mainstream Media." *Journal of the European Economic Association* 15, no. 5 (October 2017), 1025–55.

Boeddu, Gian, Jennifer Chien, Ivor Istuk, and Ros Grady. 2021. *Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches.* Policy Research Paper, April 2021. World Bank Group, Washington, DC.

Boyd, Mark, and Michel Hanouch. 2020. "Customers Want Data Protection: How Can Open API Providers Deliver?" *CGAP Blog*, April 21, 2020.

EDPB (European Data Protection Board). 2020a. "Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR." Version 2.0, adopted on December 15, 2020.

EDPB (European Data Protection Board). 2020b. "Guidelines 05/2020 on Consent under Regulation 2016/679." Version 1.1, adopted on May 4, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

European Union. 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, https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vk0vn25mntsj.

Gill, Sanjivan, and Onkar Sumant. 2020. Open Banking Market: Global *Opportunity Analysis and Industry Forecast, 2019–2016.* Allied Market Research, March 2020.

Hamilton, Philip. 2019. "'You're More Likely to Divorce Than Switch Banks': Will Open Banking Encourage More Switching?" *FlagPost* Blog, July 17, 2019, https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2019/July/Open_Banking.

Jaffee, Dwight, and Thomas Russell. 1976. "Imperfect Information, Uncertainty, and Credit Rationing." *Quarterly Journal of Economics* 90, no. 4 (November 1976), 651–66.

Leong, Emma. 2020. "Open Banking: The Changing Nature of Regulating Banking Data—A Case Study of Australia and Singapore." *Banking & Finance Law Review,* no. 35.3 (July 2020), 443–69.

Madrigal, Alexis C. 2012. "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days." The Atlantic, March 1, 2012.

McDonald, Aleecia M., Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. "A Comparative Study of Online Privacy Policies and Formats." In Privacy *Enhancing Technologies: 9th International Symposium, PETS 2009,* Seattle, WA, USA, August 2009, Proceedings, edited by Ian Goldberg and Mikhail J. Atallah, 37–55. Springer.

Medine, David, and Gayatri Murthy. 2019. "Three Data Protection Approaches That Go Beyond Consent." *CGAP Blog,* January 7, 2019.

Miller, Margaret J., Ed. 2003. *Credit Reporting Systems and the International Economy.* MIT Press, Cambridge, Massachusetts.

Montes, Fredes, and Maldonado Luis. 2020. Comparative Open Banking Frameworks; Financial Inclusion Global Initiative Symposium, World Bank.

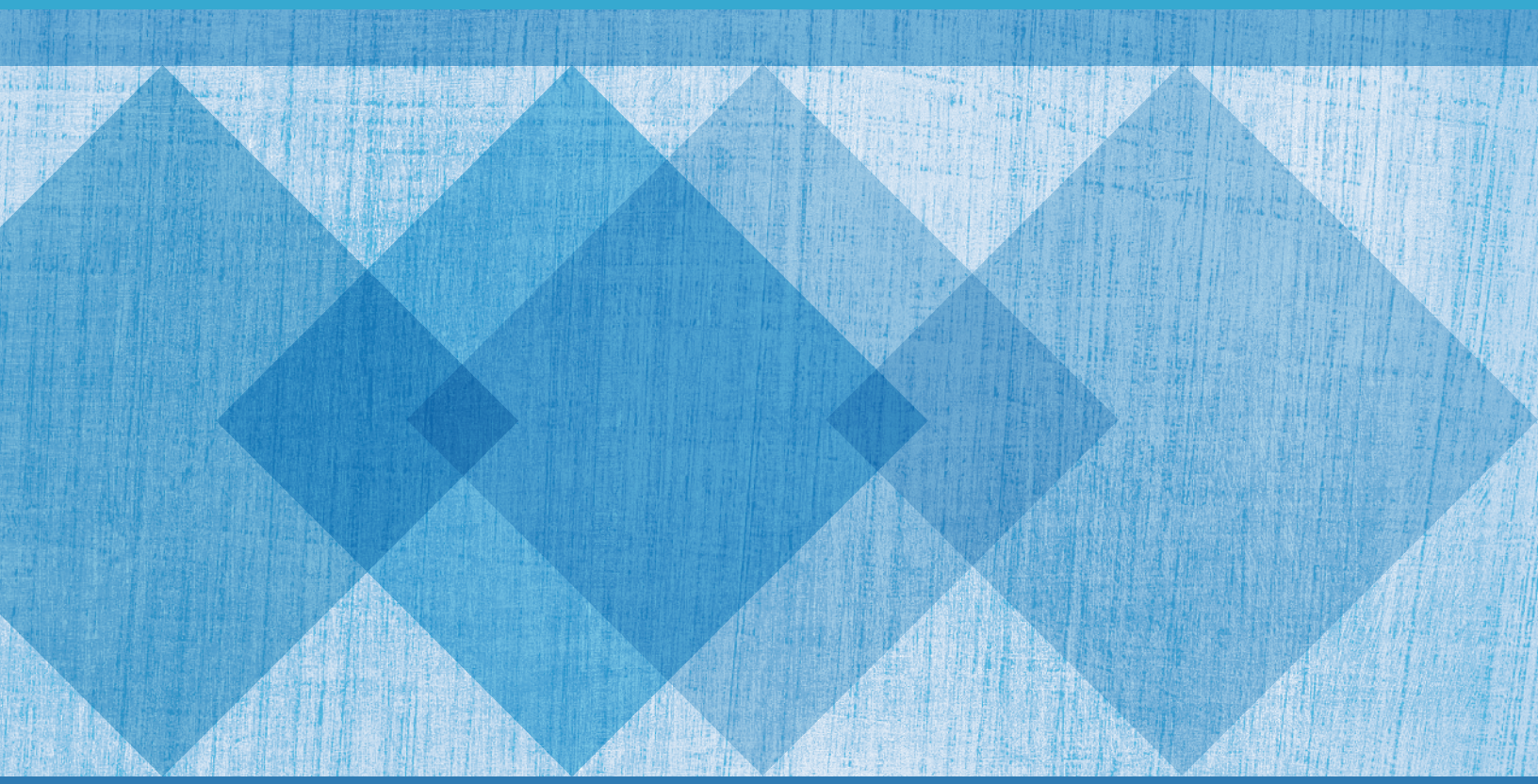
Murthy, Gayatri, and David Medine. 2018. "Data Protection and Financial Inclusion: Why Consent Is Not Enough." CGAP Blog, December 20, 2018.

ODI (Open Data Institute) and Fingleton. 2019. *Open Banking, Preparing for Lift Off: Purpose, Progress & Potential,* https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf.

Plaitakis, Ariadne, and Stefan Staschen. 2020. "Open Banking: How to Design for Financial Inclusion." Working Paper. CGAP, Washington, DC.

Stiglitz, Joseph E., and Andrew Weiss. 1981. "Credit Rationing in Markets with Imperfect Information." *The American Economic Review* 71, no. 3 (June 1981), 393–410.

WP29 (Article 29 Working Party). 2018. "Guidelines on Consent under Regulation 2016/679 Adopted on 28 November 2017 as last Revised and Adopted on 10 April 2018," https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.



WORLD BANK GROUP