DEVELOPMENTS IN OPEN BANKING

Key Issues from a Global Perspective

MARCH 2022

FUTURE OF PRIVACY FORUM

AUTHORED BY

Hunter Dorwart

Policy Counsel, Future of Privacy Forum

Daniel Berrick

Policy Fellow, Future of Privacy Forum

Dale Rappaneau

Policy Intern, Future of Privacy Forum

ACKNOWLEDGMENTS

This paper benefited from contributions and editing support from Limor Shmerling Magazanik, Managing Director, Israeli Tech Policy Institute, Zoe Strickland, Senior Fellow, Future of Privacy Forum, Lee Matheson, Policy Counsel, Future of Privacy Forum and the FPF Open Banking Steering Committee.

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org**.**

TABLE OF CONTENTS

SUMMARY

Open banking has become an influential regulatory trend in many jurisdictions.[1] Policymakers across the world have leveraged open banking tools to accomplish a wide range of goals, from promoting competition in the banking sector to facilitating innovation in financial technology services. Open banking also aims to boost financial inclusion in many countries, create new business models and services, and accelerate the financial services industry into the digital future. Policymakers are pursuing open banking to bring benefits for consumers, businesses, and governments across the world, including less costly and higher quality services, convenience, speed, new sources of value, and more competition, innovation, and inclusion.

Efforts to realize open banking's benefits must navigate a complex set of market and regulatory factors. At the heart of open banking lies the sharing of personal information, which raises a plethora of **data protection and security risks**. If unaddressed, these risks may inadvertently hinder open banking policies or implementation, create tension between different legal obligations, or result in harm to vulnerable individuals and organizations. As governments grapple with such challenges, the implementation of open banking frameworks remains a daunting task that could create significant costs and burdens for businesses and governments across the world.

Open banking frameworks vary for multiple and complex reasons. At a minimum, the **regulatory and market conditions** unique to each country often results in policymakers approaching the problem in different ways. Variation between administrative structure, regulatory organization, and legal governance in a given jurisdiction often translate into different implementation approaches in practice despite common problems faced by all regulators. Additionally, market conditions and the policy goals informed by these country-level conditions make it challenging to reconcile open banking approaches in different jurisdictions. Related to this, open banking may help solve multiple problems at the same time, yet not every country pursues the same objectives with the same policy tools in mind.

Despite this, certain commonalities are emerging between open banking frameworks. This raises important questions for how policymakers across the world can best leverage experience from other approaches and share best practices. Generally, open banking frameworks vary from narrow to broad, depending on the **definition** of open banking adopted, the **type** of regulatory model chosen, the extent of covered **services, participants, and data**, and the nature of **regulatory oversight**. Regardless of the scope of these frameworks, the interplay between open banking and **data protection law** raises important issues that must be addressed by any regulatory framework.

This report outlines issues for discussion and key findings, which are based on a survey of open banking initiatives in ten jurisdictions.[2] Each topic represents a fundamental component of open banking in many jurisdictions across the world. For each topic, the report identifies notable areas of convergence and divergence to map common issues faced by all open banking architectures, while also highlighting important nuances between such approaches. This report aims to help stakeholders better understand the key issues that generate confusion and hinder open banking practices.

KEY ISSUES AND TOPICS FOR DISCUSSION

1. Variations in Definitions of Open Banking

There is **no international consensus** on the definition of open banking. Government instruments, academic reports, and industry documents often use the term in ways that differ depending on the specific policy goals, rules, or market activity in mind. Historically, open banking included the sharing of information through numerous techniques, such as screen scraping, and did not refer exclusively to one method of facilitating or regulating data flows.

However, stakeholders broadly agree that open banking today primarily involves the **sharing of information via application programming interfaces (APIs)** between entities in the financial or banking sectors to provide new products and services.[3] Positions diverge with respect to which entities, services, and data should be included in open banking frameworks, as well as the role of the consumer, fintechs, and the larger digital ecosystem in operationalizing regulatory and market incentives for the program. These points of difference are highlighted below:

- **Some jurisdictions construe open banking narrowly to refer to the process by which a financial institution shares consumer data with a third-party upon the request of the consumer.** This approach limits the focus of open banking on encouraging large financial incumbents to share consumer data with third parties. Sometimes, this refers only to specific services, such as accounts information and payments initiation services in the UK and France.[4] Other times, conceptual definitions turn on the types of data being shared, as in Nigeria and Brazil.[5]
- **Open banking may also be broadly defined to include the sharing of data between multiple entities to provide a whole range of innovative products and services.** These definitions reflect a wider view of open banking's role in facilitating data sharing between numerous entities, such as fintechs. Open banking from this perspective not only serves to respond to consumer requests, such as for payment initiation, but also creates competitive environments where financial services can easily access data to better promote a variety of digital services. This is seen, for instance, in India, Singapore, Brazil, Mexico, Bahrain, and Australia.
- **There is a growing distinction between open banking and open finance in some jurisdictions.** For instance, in the UK, the former refers primarily to the narrow definition of facilitating accounts information and payments initiation services upon the request of the consumer, while the latter takes on a broader scope to include the innovation in financial services that results from a voluntary and open data sharing ecosystem.[6]
- **Other approaches prefer the term open data and see open banking as a sectoral subset of a larger data sharing ecosystem.** Some experts stress the need to rethink open banking even as it is being implemented due to the risk that existing frameworks reinforce information asymmetries within financial markets. Open data is one term that goes beyond traditional banking to include an economy-wide, consumer-centric right to data portability, where personal information can be shared between multiple entities. Singapore and Australia are two examples where this approach is emphasized.[7]
- **Definitions also vary depending on how open banking strategies relate to other development goals, such as financial inclusion, literacy, and maturity.** Countries with underdeveloped financial markets and infrastructure tend to approach open banking differently than those with heavily concentrated markets. These countries may see open banking as connected to larger development goals such as promoting

financial inclusion, and facilitating cross-border remittances, while others may have more limited goals in mind like making traditional banking sectors more competitive.

‹ INSIGHTS AND TAKEAWAYS ›

The lack of a definition around open banking reflects the different priorities, goals, and administrative systems of jurisdictions. Open banking is not a one-size-fits-all project. Stakeholders are recommended to keep these differences in mind to better understand their country's approach while addressing common issues faced by all jurisdictions.

At a minimum, there should be understanding across policymakers and stakeholders that open banking covers the sharing of APIs and consumer data to provide new products and services and that broader coverage reflects continued evolution.

2. Three General Approaches to Open Banking and Emerging Nuances

Sources usually place open banking approaches into one of three categories: (i) initiatives where data sharing is **required** under law ("prescriptive"); (ii) initiatives where data sharing is **encouraged** but not mandated by regulators ("facilitative"); and (iii) initiatives where the **market** drives financial data sharing ("market-driven").

A broad analysis of open banking frameworks across the world confirms that the majority of initiatives fall within these categories. Although countries differ in how they leverage existing administrative institutions to implement open banking goals, the majority fall within one of the categories enumerated above and either require or do not require covered entities to engage in data sharing pursuant to open data frameworks.

While this typology is useful to get a broad sense of the state of open banking around the world, it distorts important complexities and nuances within each country's approach. Stakeholders should therefore focus on identifying the benefits and challenges that face each type of initiative, rather than mapping general approaches. Such challenges include striking an appropriate regulatory balance, ensuring data protection and security, and encouraging innovation and consumer protection. These nuances and complexities are highlighted below:

- **Some open banking frameworks require financial institutions to share data as a matter of law**. The European Union, Australia,[8] Brazil,[9] Mexico,[10] and the UK[11] have mandatory data sharing regimes. However, these jurisdictions' frameworks differ in the types of covered services and participants, the timing of implementation, and the regulatory instruments used to effectuate data sharing.
- **Other jurisdictions encourage data sharing by issuing guidance, formulating open API standards, and/or establishing voluntary data sharing platforms.** For instance, India, Nigeria, Singapore, and Bahrain have created frameworks that fall within this category. As with the mandatory regimes above, these jurisdictions also differ in the types of covered services and participants, the timing of implementation, and the regulatory instruments used to effectuate data sharing. In the United States, the Financial Data Exchange (FDX), a non-profit developing specifications and technical standards for open finance models, has brought together stakeholders from across the financial services industry to unify common standards of data sharing.[12]
- **Some countries have taken a more light-touch approach and are now formulating rules based on best practices.** In the US, the Dodd-Frank Act requires "covered persons" to make certain information available to consumers upon request, pursuant to regulations issued by the Consumer Financial Protection Bureau (CFPB).[13] In 2020 the CFPB initiated its rulemaking process but has yet to publish final rules.[14]

- **Comparisons between jurisdictions with overlapping data sharing approaches are complicated by other issues, such as implementation.** Open banking is still in its early stages in many jurisdictions, with some regulators just beginning to formulate strategies, while others are further ahead with implementation. Many countries are still experimenting with frameworks and have delayed implementation for numerous reasons. For instance, Mexico, Australia, and Brazil have notably experienced delays.[15]
- **Open banking frameworks within each category vary in scope, requirements, and regulatory mechanisms.** Jurisdictions are not aligned in the types of services and participants covered by their frameworks. For instance, in Brazil, regulators can only require specific types of banks to participate but encourage other financial institutions to join the framework. These institutions share data on a whole range of services including insurance and capital markets and must receive certification and approval from the Central Bank to participate. This is in contrast to frameworks in the UK and France, which require banks ("account servicing payment service providers") to grant account information and payments initiation service providers access to their customers' payment accounts "on an objective, non-discriminatory and proportionate basis".[16]
- **Jurisdictions that do not mandate data sharing may impose other requirements, such as formulating or publishing APIs.** Singapore's framework, for instance, encourages entities to set APIs to be included in the country's Financial Industry Open AI Register.
- **Likewise, countries with mandatory approaches differ in the type of entities they regulate and vary in flexibility.** Australia's open banking initiative, the Consumer Data Right (CDR), is currently mandatory for entities supervised by the Federal Treasury or that have received licenses from other authorities. This includes the majority of banks and many other financial institutions. By contrast, in Brazil, only entities categorized as S1 or S2 under Brazilian banking law must participate. Both jurisdictions, however, have taken steps to encourage non-supervised entities (e.g., fintechs) to voluntarily join and receive accreditation from regulatory authorities.
- **Finally, some jurisdictions have taken relatively novel approaches that are unique to their own market and regulatory environments.** For instance, Nigeria's voluntary framework uses a "tiered" approach that allows participants to gain access to certain types of data after receiving approval from the Central Bank of Nigeria. This is similar to Brazil's "phased" implementation approach but operates on a voluntary basis. Likewise, India relies on the creation of Account Aggregators (AAs) that receive authorization from the Reserve Bank of India (RBI) to intermediate between data holders, data recipients, and consumers.[17] Finally, Singapore created an API Exchange (APIX) and Financial Industry API Register where participants can download and exchange open APIs that have been registered with and approved by the Monetary Authority of Singapore (MAS).

❮ INSIGHTS AND TAKEAWAYS ❯

While the three categories of open banking reflect broad similarities between different countries' approaches, stakeholders are recommended to be cautious of overgeneralizing and not approach open banking with a path-dependency framework in mind. More than one model can work and each model can have components of more than one approach.

Any model that suits the culture and the state of financial maturity can effectuate open banking goals and bring benefits to consumers. Regardless of the model chosen, it's important that regulators understand the technology, seek input from relevant stakeholders (e.g., industry, civil society, academia), and establish proper mechanisms to monitor implementation, evaluate trade-offs, and cooperate with other regulators where appropriate.

3. Determining Scope of Covered Services

Countries vary considerably in the **types of financial products and services** covered in open banking frameworks. Such variation reflects not only the different market and regulatory conditions of a given country's financial sector, but also the specific goals and models policymakers aim towards and have drawn from when implementing open banking strategies.

There are broad similarities in the types of covered services across jurisdictions. These commonalities typically relate to basic financial services like payments, accounts information, and certain product offerings. However, notable divergences exist in cases where open banking initiatives involve broader or narrower goals, such as when a framework extends to other sectors like health or energy or only involve one specific type of service. Additionally, many countries have adopted **different terminology** to define relevant services, which raises issues with learning and drawing best lessons from other models.[18]

- **Nearly all open banking initiatives focus on payments initiation services.** Such services involve customer-permissioned data sharing to process and complete financial transactions between entities. For instance, Pix in Brazil enables rapid execution of payments and transactions using digital technologies. Some countries (e.g., Brazil) centralize payments initiation services through a public organization, while others rely on private third-party services (e.g., United States).
- **Some countries utilize a more targeted approach that includes payment initiation and additional banking services, but excludes others**. For instance, in both the United Kingdom and Bahrain, regulators have narrowed open banking to include account information service providers (AISPs) and payment initiation service providers (PISPs).[19]
- **Other jurisdictions apply a broad scope of covered services to facilitate innovation in multiple verticals in the financial industry**. These approaches cover many types of financial services including insurance, credit, securities, and loan information, on top of payments initiation and account information services. Open banking in Brazil, India, Mexico[20], and Singapore follows this model.
- **Some jurisdictions are extending their open banking initiatives to other sectors such as telecommunications, health care, and energy.** These countries (e.g., Australia and India) tend to frame open banking within the larger trend of open data and attempt to leverage lessons from the financial sector into other industries.

‹ INSIGHTS AND TAKEAWAYS ›

The scope of services depends on the concrete regulatory goals of each open banking initiative. Some frameworks apply to a narrow category of services, recognizing that such initiatives should primarily facilitate payments or accounts services. Others take a broader approach and contemplate the transformation of multiple services. While there is agreement on some terminology (e.g., PISPs, AISPs), the majority of frameworks adopt different terms to describe different services.

Regulators are recommended to acknowledge the risks of incorporating each type of service into their open banking strategies, and take steps, such as pilot testing, to ensure that data sharing flows smoothly while remaining protected. Open banking frameworks do not need to launch all services at once but can take a gradual approach through experimental phases or stages. Regulators should not worry about how they describe such services as long as they understand their function and relationship to the larger financial industry.

Additionally, policymakers should not lose sight of the individual consumer when contemplating the types of services open banking seeks to transform. This is especially true for ambitious approaches that seek to authorize open data sharing for multiple financial verticals, such as those related to capital markets, insurance, or other investment vehicles.

4. Variety and Function of Open Banking Participants

The variety and function of participants in open banking frameworks relies on numerous factors, including the goals of the initiative, the types of services covered, and the interaction of the framework with existing regulatory architectures. While the regulatory and market environments in each country involve a unique combination of these factors, general tendencies can be seen across jurisdictions.

- **Most open banking frameworks involve two types of participants: (i) entities that share data, and (ii) entities that receive or have the right to receive and access such data**. Data sharing frameworks, whether mandatory or voluntary, involve the sharing of information between these participants. Some countries, like India, have created intermediaries to facilitate this process.
- **Participants that hold data generally include large financial institutions, banks, and other providers.** Terminology varies across jurisdictions. For instance, open banking frameworks in the UK and Australia explicitly target large banks, while regulations in Brazil include banks categorized as S1 and S2. Likewise, Singapore's initiative mentions "providers", while the EU focuses on account service payment service providers (ASPSPs).[21]
- **Jurisdictions with broader frameworks target a wider range of financial sector entities such as fintech institutions, capital markets firms, and credit bureaus**. Singapore's framework is open to participants outside of traditional banking sectors, such as those in capital markets, insurance, and other payment firms. Fintechs, clearinghouses, and other data aggregators play a data sharing role in Mexico. Nigeria takes an expansive approach and includes entities outside of traditional account information and payments services.
- **The types of data recipients and their access rights vary depending on structural factors**. These include, for instance, whether participation is mandatory (e.g., in the UK, Australia, and Brazil), whether right of access is conditioned upon licensure or authorization (e.g., in the EU, Australia, Brazil, India, and Nigeria), or whether data can be accessed upon request (e.g., in Bahrain and Singapore). Data recipients in most approaches must comply with some mandatory technical specification standards.
- **Open banking frameworks can include a broad range of different business models, such as data aggregators.** Digital technology has enabled the participation of novel businesses in the financial services industry that play a central role in facilitating data transmission across parties. While many open banking frameworks have sought to provide a direct connection between data holders and recipients, data sharing in many countries continues to rely on third parties and other services within the ecosystem. These entities occupy an important position within the larger data sharing framework in terms of facilitating the exchange of data.
- **Some regimes consider participants as both entities that share data and entities that receive data.** This is the case in Mexico, India, Brazil, and to a lesser extent Australia, where participants receiving data must also share their own with the provider. Other jurisdictions, such as Nigeria, the UK, and the EU, establish clearer distinctions, with data sharing responsibilities applying to one category of participant but not the other.

‹ INSIGHTS AND TAKEAWAYS ›

Open banking involves participants that share data or have the right to receive and use data. These two participants usually come with separate responsibilities and limitations respective of their role (e.g., data recipients can access the data for limited purposes and must adhere to minimum security standards), or a combination of responsibilities and limitations if the entity both shares and has a right to receive and use data.

Policymakers are recommended to consider how they can facilitate third parties to approach the act of receiving data. The more third parties are incentivized to actively seek and receive data from holders, the more receptive they'll be to open banking initiatives and thus work towards fostering innovation and consumer benefit.

Regulators are also recommended to consider the scope of the open banking framework when defining participants. A narrower scope may apply responsibilities and limitations only to traditional banking institutions, whereas a broader scope may apply responsibilities and limitations to credit bureaus, capital market firms, intermediaries, fintech institutions, and more.

5. Determining Types of Covered Data

Similar and related to the scope of covered services, there is broad divergence in the categories of data covered by open banking initiatives and the terminology used to describe this data. Initiatives that focus on services in the traditional banking sector, such as payments and accounts, tend to include **basic account information** like balances, registration, and **know-your-customer** data.[22] Almost all frameworks contain some treatment of **transaction data**, particularly around payments initiation, but differ widely in terms of implementation. Additionally, frameworks that construe open banking more broadly to include other sectors of the financial services industry have expanded the scope of customer and transaction data. Many of these do not mandate data sharing but actively encourage it through coordinated open API standardization and management. Similarly, jurisdictions that take a more expansive categorization of data tend to promote **open data** concepts generally and see API sharing extending beyond finance. This report highlights the following issues:

- **Most jurisdictions recognize a distinction between generic services data, consumer data, and transaction data.**[23] There are notable variations in terminology and approaches. For instance, Mexico's framework distinguishes between open data, aggregated data, and transaction data, with the first two referring to generic non-confidential banking data and non-personal statistical information based on transactions, respectively, while the latter includes personal information.[24] In Singapore, the Financial Industry API Register recognizes two categories of information: transactional data (which contains sensitive client data) and informational data (which contains non-sensitive information).[25]
- **Categorization of data differs depending on the scope of the open banking framework, the types of services involved, and the degree of API standardization.** Initiatives that focus exclusively on account information and payments initiation services (e.g., UK, and Bahrain) limit the types of consumer and transactional data in use, although in practice it is hard to identify the scope of specific kinds of personal information included in these definitions. By contrast, broader frameworks (e.g., India and Singapore), tend to provide more granular details about the data points that fall within covered data categories.[26] For instance, the Reserve Bank of India has provided an illustrative list of different types of data under the category of "financial information," although it does not define personal information.[27]
- **Personal financial data relating to an identifiable individual is almost always involved.** In theory, all open banking frameworks implicate the sharing of personal

information, which require authorization and consent from the customer.[28] Many jurisdictions have confronted implementation challenges due to the data privacy and information security concerns personal data transfers raise, as well as because of the lack of clarity around the definition of personal data. Specific design choices, particularly around the management and supervision of standardized APIs, and existing data protection laws may mitigate or complicate such challenges.[29]

- **There are variations and challenges with regard to phasing and implementation.** The majority of jurisdictions have taken a phased approach to regulating open banking data flows. Under this approach, the kinds of data that financial institutions must share depends on the level of regulatory implementation. For instance, Brazil divided implementation into four phases, each corresponding to a different type of service and data to be shared.[30] Other jurisdictions, like Nigeria, have established a tiered approach, where the kind of data participants can access depends on the participant's level of accreditation with the Central Bank.[31]

6. Variations in Regulatory Authority and Supervision of Technology

Many open banking frameworks contain features that extend to multiple disciplines and areas of regulation including data protection, information security, competition law, cybercrime, and wire fraud. This complexity often poses challenges for **regulatory coordination**, as multiple administrative authorities may play a role in addressing issues related to the sharing of consumer data between financial institutions. Each jurisdiction has taken its own approach to this issue and coordinated regulatory oversight based on factors unique to its historical environment, including legal and administrative structure, policy goals, and market conditions. Below are the notable patterns and issues related to regulatory oversight:

‹ INSIGHTS AND TAKEAWAYS ›

The data involved in an open banking framework depends on the framework's scope. A broader scope (i.e., more services and participants covered) typically increases the types of data covered, but a framework's scope can start narrow and broaden overtime to include more types of data.

Open banking usually involves information that can relate to an identifiable person. Consequently, regulators are recommended to consider data protection principles such as minimization, purpose limitation, and de-identification when scoping the types of data covered in open banking frameworks, and understand there may be tension when addressing a consumer-driven process like open banking.

Regulators are suggested to be aware that even specifying categories of information could create legal gray areas. These areas may lead companies in the data exchange framework to differ in their interpretation of the kinds of data that fall within a particular category and may hinder the maturation of open banking ecosystems. Regulators are recommended to also align open banking data classification efforts with the open API standardization process to reduce friction and the likelihood of entities sharing data not contemplated in the framework.

- **Authority can be exercised by one primary regulatory body or shared among many.** In many jurisdictions, the primary monetary authority, such as the central bank, is the main body responsible for implementing the rules of open banking and monitoring compliance.[32] Some countries, including the UK and Australia, have also opted for this single body approach. However, these jurisdictions have designated market and competition regulators to fill this role rather than a primary monetary authority[33] Other countries, such as

Mexico, have split authority among several agencies to supervise different entities in the open banking ecosystem.[34] Note that in all jurisdictions, numerous government bodies play some supporting role. For instance, in both India and the United States, regulators must consult with other counterparts when formulating rules.[35]

- **Supervisory bodies have implemented open banking frameworks largely through pre-existing legislative authority.** In most cases, the rules and regulations implementing open banking strategies come from pre-existing authority and are formulated under designated agencies' administrative rulemaking powers.[36] There are unique exceptions, including Mexico and to some degree, the UK.[37] The issue of source of authority may be related to whether a given jurisdiction has adopted a mandatory or voluntary framework. For instance, both the Central Bank of Brazil and Australia's ACCC can require these countries' largest banks to participate in Brazil and Australia's open banking frameworks respectively. However, both lack authority to mandate that other third parties join. Whether regulators have pre-existing legislative authority to supervise new entities may partially explain certain design choices and raise notable challenges for future private-sector participation.
- **Almost all regulatory authorities must accredit or certify open banking participants in practice.** This is especially true for frameworks that extend beyond traditional financial institutions and include numerous third-party providers, such as fintechs. Imposing an authorization requirement can help ensure regulatory oversight over entities that fall outside traditional supervisory authority. Some jurisdictions, like India, exercise this power by accrediting intermediaries between data providers and data recipients. Others, like Mexico, may not require data recipients to receive approval before accessing data. However, organizations that qualify as data recipients under Mexican law can usually be data providers when these organizations receive requests for certain data. In such a scenario, registration will be required.[38]
- **Supervision over third party entities may be limited, which brings risks for consumer protection and liability for banks.** Regulators may have limited if any ability to supervise third parties in cases where these parties have no prior authorization from regulators or contractual relationships with banks. In such circumstances, regulators may find it difficult to set expectations or apply consumer or data protection law to third parties. Such entities may therefore fall outside the scope of the legal and regulatory standards that apply to banks, leaving consumers potentially unprotected when personal data is shared with and subsequently reused by fourth parties. The lack of supervision also raises questions around liability sharing, such as for improper money transfers.
- **Supervision and management of APIs raises complex challenges and dilemmas for regulatory authorities.** A minority of supervisory bodies require financial entities to submit APIs for approval.[39] Regulatory bodies' role over setting API standards also varies among jurisdictions. Some bodies exercise direct influence in setting technology standards, while other institutions take a more agnostic approach.[40] Regardless, many jurisdictions impose API guidelines and/or security standards.[41] These guidelines and standards may create difficulties for open banking, since the development and maintenance of commonly accepted API standards can be costly. Regulators must therefore choose to what extent they will invest in maintaining open API registries and setting specifications.
- **Open banking also poses novel conflict of law scenarios.** These conflicts may arise both between and within jurisdictions and create legal uncertainty. For instance, contracts between banks and third parties may indicate that one country's open banking rules apply, while the site of the transaction may impose different rules. Cross-border payments between banks with subsidiaries in multiple locations may also present new challenges for legal compliance, given extensive and conflicting financial regulations across the globe.

‹ INSIGHTS AND TAKEAWAYS ›

Despite common patterns in regulatory oversight, each jurisdiction has nuances that make it difficult to identify best practices. Each jurisdiction's unique historical and legal conditions have given rise to considerable differences in the level of administrative supervision. When drawing the best lessons, policymakers are suggested to identify aspects of their market and regulatory conditions that correspond to those faced in other jurisdictions and articulate the best pathways to achieving regulatory goals.

While there is no universal answer on the best regulatory model, a few recommendations stand out. First, authorities (including those responsible for data protection law) are recommended to collaborate to clarify regulatory roles to minimize administrative conflict and streamline business registration, monitoring, and supervision. Coordination is even more critical in the open banking context, since its purpose and success depends on inter-connection and data exchanges between stakeholders. Lastly, authorities are suggested to consult with experts to better understand the APIs they supervise to prevent technology failures, design flaws, or misleading interfaces, and consider the most appropriate liability-sharing frameworks given unique market conditions.

7. Interaction and Emerging Complexity with Data Protection Laws

The interaction between open banking and data protection law raises complex questions and novel challenges for regulators. Most jurisdictions have standards for **data processing, transmission, and storage** as well as other security requirements for financial institutions. Because open banking involves the sharing of personal data, often at the direction of the individual consumer, policymakers must ensure that guidance and implementation of such frameworks is not only consistent with data protection standards but also does not impose burdensome costs to market entities by creating additional legal uncertainty.

Jurisdictions with open banking frameworks have taken a variety of approaches to address these issues. Many of them have already adopted or plan to update existing data protection laws. In some circumstances, data protection authorities have **released guidance** on the interplay between open banking frameworks and data protection law. While a useful first step, many jurisdictions still have not clarified relevant issues. Below are the key challenges and topic areas for discussion:

› **Maintaining consistency and providing clarity around consent rules is a key challenge and priority.** Many open banking frameworks explicitly require the consumer's authorization to initiate data sharing, without defining consent or outlining conditions for its validity.[42] In these circumstances, understanding the interaction of these frameworks with data protection law becomes critical to avoid regulatory confusion and conflicting obligations.[43] Clarity may be needed around the scope and necessity of obtaining consent and raise issues such as:

- Consent rules vary across jurisdictions, which raises problems for interoperability across borders. Despite similarities in some open banking frameworks, conditions of valid consent differ considerably between the data privacy regimes of many jurisdictions.[44]
- Subsequent transfers or reuse of personal data by additional third parties may fall outside the scope of consent. This is particularly problematic in circumstances where consent rules around reuse are unclear, undefined, or underenforced. Lack of clarity may pose an increased risk of harm to individuals.[45] In Europe, the PSD2 forbids PISPs and AISPs from processing payment data that these third parties access from banks for purposes other than the provision of their own services.[46]

- Consent may apply to different types of processing and different recipients. Under both open banking and data protection law, banks may use different technical features (i.e., pop-up windows) to obtain consent or authorization from consumers, but may differ in the granularity of notice provided to the consumer. Because open banking models involve consumer-directed authorizations, a binary, yes-no consent model raises issues regarding how far consent relates to multiple types of processing such as use, sharing, or both and to which recipients the consent applies to.
- Open banking also raises issues with the expiration or withdrawal of consent. Many data protection laws impose rules on organizations regarding the expiration or withdrawal of consent. Open banking scenarios may raise further complexities around obligations of banks if consent is revoked.
- Digital IDs or other authorization tokens may be adopted to facilitate oversight. Some jurisdictions have addressed consent problems through integrating existing national digital identification programs into open banking frameworks. For instance, open banking in Singapore and India partially root authentication of consumer consent to relevant digital IDs (e.g., SingPass and Aadhar).
- Some jurisdictions have created their own consent management platforms to authenticate consumer authorization. Account Aggregators (AAs) in India serve this function and are directly supervised by the Reserve Bank of India (RBI). AAs respond to data sharing and access requests from financial institutions by validating and authenticating consent artifacts with the individual consumer. India's open banking rules provide detailed notification and consent requirements for financial institutions when developing these artifacts.

› **While open banking frameworks may help implement data portability principles, these frameworks could fail to effectuate this and raise market symmetry challenges.** Many data protection laws recognize a data subject's right to data portability, or the ability to have a person's data transferred from one entity to another.[47] Open banking frameworks present the opportunity to implement data portability in practice and further align existing data protection standards with novel business and regulatory models. However, many jurisdictions have recognized the need to ensure reciprocity between recipients of data and data providers.[48] Challenges remain in specifying what reciprocity means in practice and whether the concept necessitates data to be shared in similar formats or quantities.

› **Financial information may fall within special or sensitive categories of personal information and therefore carry more risk in transmission.** Some data protection laws treat financial information as sensitive or deserving of heightened processing restrictions.[49] Due to the nature of this information, open data sharing may place the individual in a precarious position, especially if numerous third parties can subsequently transfer and reuse such data. The interplay of such restrictions with open banking frameworks remains unclear.[50]

› **Data localization rules may hinder the efficacy and implementation of open banking.** Some jurisdictions are considering localization rules for financial information.[51] These rules may frustrate the goals of open banking as localization would create costly procedural hurdles that may prevent data sharing across borders and between banks and foreign subsidiaries. To ensure that banking data crosses borders, some countries have partnered with other jurisdictions to create test pilots for payment initiation and transactions processing utilizing open APIs.[52]

- **Open banking raises numerous implications for data and cybersecurity, such as data breach obligations.** Many data protection laws require certain entities to meet minimum technical and organizational requirements to ensure security in the processing, transmission, and storage of data. Other security-related laws focus on data breach notification requirements, and may impose liability for failure to meet them. Security risks related to open banking should be carefully considered, whether in terms of required additional controls, responsibility among parties exchanging data (such as relating to data breaches or fraud), and consumer expectations and understanding that impact reputational risk.[53]
- **Regulatory bodies may need to coordinate to ensure consistent enforcement and clarity around grievance mechanisms.** Many data protection laws require data processors to establish grievance mechanisms for individuals to exercise data subject rights or file complaints. Open banking frameworks that impose similar legal obligations on financial institutions are recommended to consider whether data protection laws' existing redress mechanisms would give rise to conflicting rules or procedures.

‹ INSIGHTS AND TAKEAWAYS ›

Financial regulators are rightly focused on safety and soundness of financial systems. Open banking requires addressing opening the system in innovative ways that raise a variety of risks, including relating to privacy and security. Data protection law has considerable implications for open banking operations. Issues related to consent, data re-use and sharing, localization, and security reflect uncertainties surrounding the relationship between open banking and existing legal frameworks.

When facing issues raised by the interplay of data protection and open banking, regulators are recommended to be more specific in addressing key challenges by leveraging expertise from industry, civil society, and academia, and not take the success of open banking for granted. While open banking promises to bring tremendous market benefits, it may not always fulfill its intended impacts if there is burdensome regulatory confusion, or consumers experience harms that they may not have expected or could have been mitigated.

To this end, regulators are suggested to keep risks and benefits to the individual consumer in mind when navigating these issues.

CONCLUSION

An analysis of key open banking frameworks around the world indicates that jurisdictions have taken a variety of approaches to address open banking goals and risks, each reflecting unique local market and regulatory conditions such as the maturity of financial markets, the level of financial inclusion, and the role of technology.

Three themes are worth highlighting. First, there is a need for regulators to address operational friction among players arising from inconsistent or vague principles, obligations, and goals. If unaddressed, the key challenges of open banking may raise costs for businesses and consumers and mire the financial ecosystem in regulatory confusion. Regulators are recommended to strive to resolve ambiguities arising from the relationship between open banking and data protection law, which make it difficult for banks and other financial entities to understand their data processing obligations. Such clarification could help ensure that stakeholders prioritize consumer benefit.

Second, there is no key model for open banking. Variations in different countries' frameworks reflect unique regulatory cultures, policy goals, and levels of financial development. Policymakers are suggested to be mindful of these differences when addressing technical and regulatory challenges, but ultimately choose a path that is best suited to their legal and economic environments. More than one model can work if coordination and engagement addresses key operational challenges and risks.

Third, policymakers are recommended to view open banking in the larger context of digital development. While open banking can solve a whole range of problems, it is its connection with innovative digital technologies and solutions that promises to transform the financial industry. Regulators are recommended to keep in mind that technology is an evolving process and that the open banking architectures constructed today will influence the stage of innovation in the future. To this end, open banking models are suggested to be flexible to not stifle future innovation while robust to keep the interests of the consumer at heart.

GOVERNMENT DOCUMENTS REFERENCE GUIDE

Australia

- Consumer Data Right
- Consumer Data Standards

Bahrain

- Central Bank of Bahrain and Financial Institutions Law 2006
- Open Banking Module of CBB Rulebook
- Personal Data Protection Law

Brazil

- Circular No. 4,015 of May 4th, 2020, Regulation on Open Banking
- Joint Resolution No. 1 of May 4th, 2020, Regulation on Open Banking

European Union

- Directive (EU) 2015/2366 (Payment Services Directive 2)
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR
- Regulation (EU) 2016/679 (General Data Protection Regulation)

France

- CNIL White Paper, *When trust pays: today's means of payment today and tomorrow to the challenge of data protection*
- PSD2 API V1.6

India

- Account Aggregator Master Direction

Mexico

- Article 76 of the Law to Regulate Financial Technology Institutions
- CNBV Regulation
- Regulation 2/2020

Nigeria

- Issuance of Regulatory Framework for Open Banking in Nigeria
- Nigeria Data Protection Regulation 2019
- Release of Consumer Protection Framework for Banks and Other Financial Institutions Regulated by the Central Bank of Nigeria

Singapore

- API exchange
- Financial Industry API Register
- Personal Data Protection Act 2012
- Singapore Financial Data Exchange
- Singpass

United Kingdom

- Payment Services Regulation 2017
- Retail Banking market Investigation Order 2017

United States

- Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) Section 1033
- Gramm-Leach-Bliley Act of 1999 (GLBA)
- CFPB Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation
- CFPB 2020 Notice of Proposed Rulemaking: Consumer Access to Financial Records
- OCC/FRS/FDIC 2021 Proposed Interagency Guidance on Third-Party Relationships: Risk Management

ENDNOTES

1 Broadly, open banking refers to the practice of allowing financial services entities to access consumer and other financial data to provide new types of products and services. Definitions notably vary between countries, with no international agreed upon approach.

2 These include the United Kingdom (UK), France, Nigeria, India, Brazil, Mexico, the United States (US), Australia, Singapore, and Bahrain.

3 *See e.g., Open Banking, Data Sharing, and the CFPB's 1033 Rulemaking*, Congressional Research Service IN11745 (2021); *Open Banking Ecosystems and the Need for a New Connectivity Model*, Kapronasia (2021); *Report on Open Banking Application Programming Interfaces (APIs*), Bank of International Settlements (2019).

4 The Payment Services Regulations 2017 (PSR); see also Directive (EU) 2015/2366 (Payment Services Directive 2) (PSD2).

5 Nigeria divides open banking participation into four tiers that correspond to types of data made available to third parties. Similarly, Brazil implemented its open banking framework in four stages, each corresponding to a type of service and data used. Central Bank of Nigeria, *Open Banking Framework*; Banco Central do Brasil, *Regulation on Open Banking* (2020).

6 See UK Financial Conduct Authority, *Call for Input*, Open Finance, (2019), 3, Accessed February 25, 2022, ("Open finance refers to the extension of open banking-like data sharing and third-party access to a wider range of financial sectors and products.").

7 Regulators intend to expand Australia's Consumer Data Right (CDR) and Singapore's API Exchange (APIX) to other sectors like telecommunications and energy.

8 Consumer Data Right, Australian Competition & Consumer Commission, Accessed March, 2, 2022.

9 Alin Popa, *Open Banking in Brazil: All Questions Answered by the Central Bank Brazil*, The Paypers (2021).

10 Greenberg Traurig, *New Open Banking Regulation in Mexico*, (June 16, 2020), Accessed February 28, 2022.

11 Deloitte Legal, *Compare Jurisdictions - Fintech Questions, The Legal 500, Accessed February 28, 2022*, (noting that "[the UK's Payment Services Regulation] provide[s] that an account servicing payment service provider – that is, the payment service provider maintaining a payer's payment account – must allow access to AISPs and PISPs").

12 Financial Data Exchange.

13 Section 1033 of the Dodd-Frank Act (DFA).

14 *Open Banking, Data Sharing, and the CFPB's 1033 Rulemaking*, Congressional Research Service IN11745 (2021).

15 Isabel Cabrero, *The State of Open Banking in Latin America in 2022*, Belvo, (January 13, 2022), Accessed February 28, 2022.

16 Article 36(1) of PSD2.

17 Malavika Raghavan & Anubhutie Singh, *Regulation of Information Flows as Central Bank Functions*, Central Bank of the Future Conference Future of Finance Initiative (2020).

18 For instance, the EU PSD2 covers all "payment services" which are listed in Annex I of the Directive.

19 Markos Zachariadis, *Data-Sharing Frameworks in Financial Services: Discussing Open Banking Regulation for Canada*, Global Risk Institute, 10 (2020), Accessed February 28, 2022.

20 Ariadne Plaitakis and Stefan Staschen, *Open Banking: How to Design for Financial Inclusion*, CGAP, 10 (2020), Accessed February 28, 2022.

21 PSD2 Article 4(17) defines ASPSPs as "a payment service provider providing and maintaining a payment account to a payer."

22 This includes every jurisdiction that mandates data sharing through a regulatory or legislative framework (e.g., UK, Brazil, Australia), but also many that have taken a more facilitative approach (e.g., Singapore). Note, prescriptive models mandate open banking precisely to require sharing of this type of data for certain banking services.

23 Generic services data relates to publicly-available information about financial products and services, such as product pricing. Consumer data relates broadly to personal client data such as overdraft information, loans, personal lines of credit, working capital, financing information, and identification information like account numbers, types of products under contract, and powers granted to representatives. Transactional data includes, for instance, deposit and savings accounts, balances, credit and debit transactions, operation identifiers, values, dates, recipient information, authorized transactions, credit availability, etc. Note, not every jurisdiction includes all types of data listed above.

24 Alejandro Landa Thierry, *Open Banking Has Arrived in Mexico*, Holland & Knight, (July 22, 2020), Accessed February 28, 2022.

25 Monetary Authority of Singapore, Financial Industry API Registry (last accessed, February 27, 2022).

26 This is also the case in Brazil, which combines both a mandatory and voluntary scheme. In May 2020, the Central Bank of Brazil published a Circular to clarify the scope of data and services. In particular, the Circular provides a list of information covered in each phase of open banking implementation.

27 The Master Direction covers "financial information" which includes: bank deposits and accounts, deposits with NBFCs, structured investment product, commercial paper, certificates of deposit, government securities, equity shares, bonds, debentures, mutual fund units, exchange traded funds, Indian depository receipts, CIS units, alternate investment funds, insurance policies, pensions, units of infrastructure investment trusts, units of real estate investment trusts.

28 Many jurisdictions, such as Mexico's, openly contemplate the sharing of transactional data, which is personal information.

29 For instance, the Monetary Authority of Singapore (MAS), oversees the authentication of APIs listed in the Financial Industry API Register. Similarly, in Brazil, the Central Bank of Brazil accredits the APIs of financial institutions.

30 Phase 1 covers product and services offered by banks, Phase 2 covers personal financial data, Phase 3 covers payments initiation information, and Phase 4 covers insurance and investments. Regulators anticipate participation in Phase 4 by May 2022. See Banco Central Do Brasil, Joint Resolution (2020).

31 See Central Bank of Nigeria, Regulatory Framework on Open Banking (2021).

32 This is the case, for instance, in Brazil, India, Singapore, Nigeria, and Bahrain. In the EU, banking authorities also share primary regulatory oversight, but cannot interfere with the competence of Data Protection Authorities to oversee payment service providers' compliance with the GDPR when implementing data sharing.

33 In the UK, the Competition and Markets Authority (CMA) is the primary regulatory body for open banking, although the Financial Conduct Authority (FCA) also has an active role in administering and regulating the UK's framework.

34 The National Banking and Securities Commission (CNBV) and the Mexican Central Bank (BANXICO) are the primary regulatory bodies, with the former overseeing data providers and data requesters while the latter sets interoperable API standards for credit reporting agencies, clearinghouses, and Recognized Entities. Carlos R. Garduño and Carlos M. Escandón, *New Open Banking Regulation in Mexico*, The National Law Review, (June 16, 2020), Accessed February 28, 2022.

35 In India, for instance, the Insurance Regulatory and Development Authority (IDRAI), the Securities and Exchange Board of India (SEBI), and the Pension Fund Regulatory and Development Authority (PRFDA) have all agreed to allow their regulated entities to participate in the RBI's AA programs. In the United States, the Dodd-Frank Act explicitly requires the Consumer Finance Protection Bureau to consult with other regulators like the Federal Trade Commission, the Federal Reserve Board of Governors, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation.

36 In Bahrain, Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 grants the Central Bank of Bahrain (CBB) the authority to formulate and implement data sharing rules between financial institutions.

37 Article 76 of the Law to Regulate Financial Technology Institutions (FinTech Law) empowers and provides guidance to Mexican authorities on how to implement open banking rules. Similarly, the UK passed the Payment Services Regulation (PSR) in 2018, which transposes the EU's PSD2 into domestic law.

38 Carlos R. Garduño and Carlos M. Escandón, *New Open Banking Regulation in Mexico*, The National Law Review, (June 16, 2020), Accessed February 28, 2022.

39 This is the case in Brazil, which requires data holders and recipients to submit APIs to the Central Bank for approval before using them to share data. SICs and clearinghouses must obtain BANXICO's approval before using aggregated and open data APIs. Approval requests must contain certain information from the Annexes, as well as other information, such as the kind of data that will be exchanged using the API.

40 For instance, India's Reserve Bank Information Technology Private Limited (ReBIT), a wholly-owned subsidiary of the RBI, has created a core set of technical specifications for adoption by all regulated entities. Similarly Singapore's MAS has released technical guidelines and standardized APIs through its Financial Industry API Register under a phased and consultative approach. In Australia, the Data Standards Body has released a comprehensive list of Consumer Data Standards which serve as the technical basis for data sharing between banks and other financial institutions. By contrast, open banking frameworks in France rely more on private-sector design and standards-setting.

41 In Mexico and Bahrain, for instance, data recipients and holders must develop open APIs per prescribed specifications and standards.

42 In the majority of these cases, a data protection bill already exists in the jurisdiction in question, which implies that relevant consent rules should be located there. However, many open banking frameworks do not specify that participants should defer to data protection laws, nor provide any direct reference to provisions or other regulatory documents. This is the case, for instance, in Brazil, Nigeria, Bahrain, and Mexico. In the UK and EU, the European Data Protection Board (EDPB) has issued guidance on the interplay between the PSD2 and the EU's General Data Protection Regulation (GDPR), but questions still remain regarding implementation.

43 Sebastião Barros Vale, PSD2, *GDPR and Banking Secrecy: What Role for Consent?*, Lexology (2019).

44 While there are broad similarities in definitions and approaches to consent in data protection laws that were modeled off of the EU GDPR, countries have varied considerably in the types of information controllers must notify data subjects before they become informed, and the scenarios (i.e., bundling, withdrawal) where consent is no longer freely or voluntarily given.

45 Some jurisdictions, like India, have established rules limiting transfer and processing explicitly in open banking frameworks, while others defer to applicable data protection law and guidance.

46 PSD(2) Art. 66(3)(g) and 67(2)(f). The implication is that such service providers cannot rely on the compatibility test under Article 6(4) GDPR.

47 The EU GDPR and Singapore's Personal Data Protection Act (PDPA) are two examples where data portability is an explicit right under law.

48 Australia's CDR explicitly requires open banking participants to share data equally. This is also witnessed to some degree in Brazil, and Singapore. While Mexico's open banking framework does not mention reciprocity outright, in practice something approximating this standard is required because the CNBV considers many data recipients to be data holders, which means they must share data upon request when the requester is acting as a provider. By contrast, the UK's PSR and the EU's PSD2 does not recognize the principle of reciprocity: data recipients are not normally obligated to make their data available to providers.

49 The draft Data Protection Bill (DPB) in India, for instance, considers information relating to an individual's finances or financial status as sensitive. Although not surveyed in this report, China, Indonesia, and the Philippines also treat financial information as sensitive data.

50 The EU PSD2 anticipates this by forbidding banks from sharing (and PISPs and AISPs from requesting/storing) "'sensitive payment data', meaning data, including personalized security credentials, which can be used to carry out fraud." This does not include the customer's name and account number. See PSD2 Art. 4(32), 66(3)(e) & 67(2)(e).

51 For instance, India's draft DPB may currently require localization of certain financial information.

52 This is the case between Singapore, India, and Indonesia.

53 Bahrain's Open Banking Module imposes additional security measures on open banking participants including auditing and reporting requirements, logs of relevant information such as technology architecture, logical security measures and mechanisms, and the security of account information and payment initiation processes.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org