Regulatory Aspects of Open Banking: The Experience thus Far[42]

by Harish Natarajan[43]

Abstract: This article discusses the emerging experience on regulating open banking, and presents some forward looking considerations around the ongoing shift from open banking to open finance to open data, impact on competition, and consumer protection.

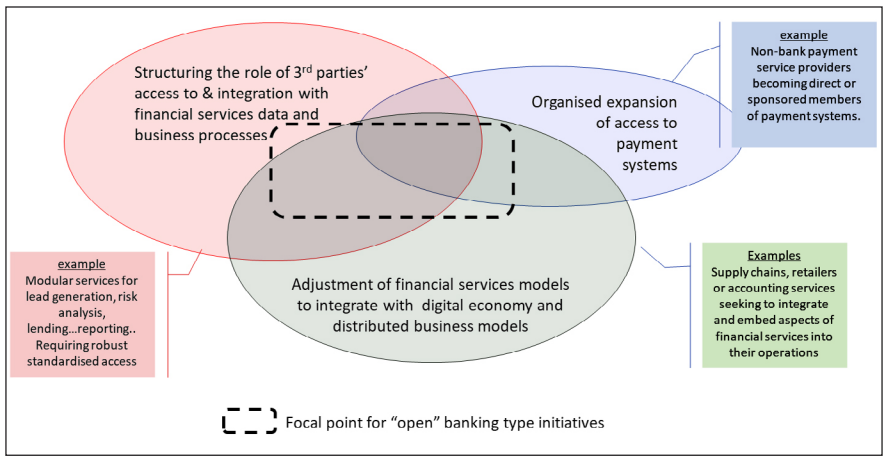
Open Banking[44] as a terminology was introduced in the UK, as a regulatory initiative following a series of investigations on enhancing competition in the banking sector. Starting with the Cruickshank report in 2000, and more proximately the Fingleton report[45] in 2014, which called for banks publishing customer data using open data constructs. A somewhat earlier parallel development was "Screen Scraping" that used system-based interfaces to "scrape" data from internet banking and other online financial services to develop useful products and services – Yodlee in the US, was one of the earliest such offering. "Screen scrapping" has been associated with concerns on data security and privacy protection, given that the third parties are essentially handling the customer credentials and as such operated in an unregulated zone. In this context[46], open banking has emerged as a system to give

42. "The views expressed in the article are the authors personal opinions and not representative of the World Bank's management or board of Directors."
43. World Bank.
44. This article is based on a presentation made by the author at an event. The presentation benefitted from the support of Fredesvinda Montes (World Bank) and Ivan Mortimer Schutts (International Finance Corporation).
45. September 2014, "Data Sharing and Open Data for Banks: A report for HM Treasury and Cabinet Office"
46. Adapted from, "Regulatory Approaches to Open Banking", World Bank, 2020.

customers the right to share with third parties they trust with their banking data and information in a secure manner and to opening and unbundling processes and services in banking sector and boost competition.

More generally, there is a broader context of *three intersecting trends* in the real sector and financial sector which has motivated open banking initiatives. The *first trend* is one of integrating third parties into business processes in the financial sector. Notable examples including lead generation, risk analysis, and data analysis. All of which require access to structured and standardized access to data and ability to trigger or initiate specific business processes. The *second trend* is to integrate financial services into new business models engendered by the digital economy. The notable example includes deep integration between financial service providers system with the accounting and financial management systems of businesses. The *third trend* is one of expanding access to payment systems for non-bank payment service providers given their increasing relevance in the payments market. Open banking lies at the intersection of these broader trends – see figure 1.

Figure 1: Open banking lies at the intersection of trends in the real sector and financial sector



This consent-based access to data and the potential communication that it allows open great opportunities for innovation, however it is also raising several policy considerations. The main objectives pursued by regulatory frameworks that define open banking are generally around encouraging innovation and fostering competition, resulting in new products and services at competitive prices to the benefit of consumers, while minimizing the risks and mitigating them, and as such striking the right balance. The below table summarizes the opportunities that accrue to the different stakeholders and the challenges that they encounter.

Table 1: Challenges and Opportunities of open banking[47]

	BANKS	FINTECH COMPANIES	CONSUMER	REGULATORS
Opportunities	New business models New revenue streams Deep customer insight More user-centric solutions	Enables ecosystem development New business models Collaborative business models with banks Scale faster	Wider range/ choice of services Improved user experience Lower prices Financ ial inclusion	More stable exchange of information Enhanced security Potent ial for suptech solutions
Challenges	Need to develop API infrastructure (cost and time) Competition and revenue loss New d istribution of liability Business model risk Customer disintermediation Cybersecurity	Security Compliance	Privacy Data security	Need to have technical capabil ities to analyze APIs Need to resolve conflicts between banks and TPPs Coordination among regulators

From a regulatory perspective, open banking should also be seen in the context of ongoing efforts by regulators to adjust the regulatory framework to create space for new entrants to provide financial services in multiple ways,[48] notably – e-money issuance and digital bank license. E-money licenses has been leveraged by telecom operators in Emerging Markets and Developing Economies

47. World Bank, Open Banking Regulatory Approaches - Technical Study on Regulatory Approaches for Open Banking
48. World Bank, Fintech and the Future of Finance, 2022.

(EMDEs) notably in Sub-Saharan Africa, although also in other regions. As the e-money providers have reached a certain scale, they are keen to pursue opportunities to expand their offerings and are entering into partnerships to offer products and services of banks and other financial service providers to their customers, often leveraging Application Programming Interfaces (API) based data exchange and transaction initiation. The development of digital banks is bringing in new entrants who start with a narrow product suite and are exploring a similar business model. Some of the digital banks are also pursuing a "Banking as a Service" (BaaS) model wherein they seek to be the gateway to a broad range of banking services that fintechs and other financial institutions can use to strengthen and expand their own offerings. BaaS models also make extensive use of APIs. In some jurisdictions the e-money providers have sought digital bank licenses on their own or in partnership with other technology partners. Open banking could in some ways open an alternate pathway for the e-money providers to expand their products and services, and at the same time BaaS while in some sense an alternative to open banking could also complement open banking by going beyond the set of APIs in the open banking remit.

Open banking raises broadly three sets of policy questions for regulators. The first is on how to foster and harness the positive impacts on competition and innovation; the second set relates to data protection and privacy; and the third is on whether and how to regulate the third parties who will now have access to customer data.

Competition and Innovation

Open banking can enable new entrants to offer more tailored and compelling services thereby expanding the range of products and services with knock on effects on competition, innovation, efficiency, and financial inclusion. The incumbents can also harness open banking to more efficiently onboard customers and offer integrated services. Globally, regulators have had to grapple with a range of questions in their quest to harness open banking for advancing competition and innovation. The key questions include: (i) **Who**: which incumbent institutions should be obliged to open access; and (ii) **What**: what types of information and services can be accessed.

On question of "who" – some regulators have required only the dominant banks (for e.g., UK, and Brazil); some have mandated it for all banks (e.g.,

Mexico); and others have expanded the scope to include all types of financial institutions (for e.g., Mexico and India). On the question of what – in general, there are two types of access – read and write. The former relates to being able to access information and the latter to also initiate transactions and in that sense modify the data. There is also a further distinction being made in some jurisdictions on product and service level information, anonymized aggregate information, customer demographic and other "static" information, and customer transaction level information. On both the questions, some jurisdictions have adopted a phased approach. Many jurisdictions that started with only banks have started expanding the coverage to cover the entire financial sector – and in that sense being more "open finance".

There is a related question to the "who" and "what", which is **how** the access is to be structured and under what terms. This question has been the most challenging given that it spans the spectrum of technology, operational and business model aspects. On the technology and operational model front, the overarching architecture and mode of access is a key decision. Globally, there are broadly three different architectures have been observed[49] – (i) centralized – with a central entity acting as a bridge between the data providers and receivers; (ii) de-centralized – with data providers and receivers establishing linkages on their own; and (iii) hybrid – which uses some centralized elements like establishing a trust framework and then leaving the providers and receivers to discover and consume the services using the trust frameworks. In general, the centralized and hybrid approaches have been more common in jurisdictions that have regulated open banking. Beyond the interface models described above there are of course issues related to data format, customer authentication and consent management processes, and service quality. On the business model – the fundamental question is should the open banking services be priced and if so at what level. Some jurisdictions have left the process of determining the technology and business model aspects to the private sector. Others have made some choices specifically on the technology and operational model – for e.g., Korea and Turkey (centralized); and Europe (hybrid). In India, where the hybrid model has been

49. BIS, "API Standards for Data Sharing", 2022

chosen, there is an added element of creating a new category of entities "account aggregators" who come in between the data providers and receivers and act on behalf of the data subject.

The question of pricing has been a very difficult issue to address. On the one hand, the data providers incur costs in maintaining the data and the associated IT systems and as such incur real costs in providing the service. On the other hand, the customers have a legitimate right to their data and a high price could act as a barrier to development of open banking. Further, in the absence of some organizing entity arriving at an acceptable price is a challenge. The centralized model seeks to resolve this through the central entity playing that role – for e.g., NPCI in India plays this role for payment initiation services. The hybrid model could also lend itself to such approaches. In general, the interchange structure followed in the payment card industry and the pricing models seen in credit reporting markets could prove relevant for open banking as well. In this regard, it is worth noting that both in the centralized and hybrid models, the central entity administers key functions akin to say a "payment scheme" or a credit bureau. This leads to the question of whether these central entities should be regulated as financial infrastructures.

It needs to be noted that while open banking seeks to expand competition, without adequate safeguards competition could actually get further weakened[50]. There is also an increasing realization that while open banking was not necessarily designed with BigTechs in mind, they are however likely to benefit significantly from this. It is becoming clear that BigTechs, given their strong customer base and apps that are integrated into daily lives of end-users, can derive significant benefits from open banking – for example in India, big techs were able to leverage the third-party payment initiation capability to rapidly expand their presence in the payments market, prompting the imposition of volume caps[51]. This has also prompted calls for introducing the principle of reciprocity and requiring the third parties that access open banking services to also themselves being obliged to open access. This however poses several issues starting from the scope of the data extending

50. Adapted from World Bank, Fintech and the Future of Finance, 2022.
51. No single third party application can exceed a market share of 30% by payments volume.

beyond the financial sector domain and challenges in standardizing. There is broad movement towards taking an open data approach, wherein the data subject is vested with the right to access and share their data held with any entity – the Customer Data Rights initiative in Australia goes in this direction.

Data Protection and Privacy[52]

Open banking is an economic reform premised on processing personal data, with consumer consent. While open banking increases transparency in financial markets by making data more widely shared, it also creates concerns about personal data protection and privacy. The use of such data could vary from enabling Third-Party Providers (TPPs) to offer payment-initiation services to comparators that use account information to compare services and products offered to a specific consumer from different service providers. As more sources of data are used to understand financial behaviors, data protection and privacy have gained even greater importance. 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.

The range of data-protection and privacy considerations under data-sharing scenarios includes data-protection principles, data governance and enforcement, and data security, including cybersecurity. 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. 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). In this context, consent of the customer is a key construct for safeguarding the interests of the customer. As such 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. 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-

52. Adapted from "Role of consumer consent in open banking", World Bank, 2021.

protection laws provide general requirements on consent clauses but may not fully reflect the technology and market conditions present in open banking.

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. 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).

In addition, several overarching consumer protection considerations also apply and need to be accounted for in open banking context. Notably, 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 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 addition, broader discussions around the potential negative consequences resulting from inadequate safeguards around data analytics and algorithm development are relevant consideration in the context of open banking as well.

The below table summarizes the key policy considerations pertaining to data protection, privacy and more broadly consumer protection in the context of 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
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, potent ial 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); ut ilize 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

Regulating third parties

Open banking regulations introduce new categories of regulated financial institutions. The PSD2 model of introducing two new categories of institutions – the Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP) – has been widely adopted across the World. There is however some variation on the approaches related to application of prudential requirements, financial conduct requirements, and supervisory approaches. An alternate model in India – is one of not regulating the PISP and instead treating it as a specific product offered by a regulated payment system through its partner banks/payment institutions and relying on the operating rules and procedures of the payment system to achieve the regulatory outcomes. On the other hand, a new category of entities called "Account Aggregators" is introduced, who act as a "data fiduciary" orchestrating the data requests from institutions that have a legitimate interest and the providers of information, and the consent of the data subject. This model while like AISPs at first glance, in reality represents a different regulatory approach. Notably, it does not pre-judge the type of services the data receivers will offer, and allows all institutions regulated by any of the financial sector regulators in India and the Department of Revenue, Government of India to be able to participate as data receivers.

Forward Look

Finally, while some topics have not been incorporated into any regulation yet and hence are beyond the scope of this article, they are on the agenda for discussion in many countries. The role of bigtech firms in the data economy, the extension of data sharing to other sectors of the economy (referred to as "smart data"), or potential efforts toward international interoperability are examples of issues that will very likely have the attention of regulators in the near future.

As described in this article, open banking is to a great extent about ecosystem creation and the smart use of data to deliver new products to customers and to encourage competition. There is no single model or solution to achieve these objectives. The models summarized in this article differ in

their approach and scope, in the strictness of the standards or principles defined, and in the definition of the responsible governing bodies, among other things. Some early lessons from the experience thus far on open banking regulations, include:

- The technology, operational, and business model issues are critical for open banking issues to be successful. While regulatory frameworks, rightly do not delve too much into these aspects, they should at the minimum foster development and adoption of standards and industry wide co-ordination mechanisms. Leveraging existing industry bodies and market infrastructures like payment systems and credit reporting systems would be relevant. Regulators however need to ensure that they are able to influence and shape the governance arrangements to ensure that the intended public policy objectives are achieved.
- The full life-cycle aspects of an open banking transaction need to be considered. For e.g., what happens to customer disputes for an open banking-initiated transaction or when a consent needs to be revoked.
- Authorities should support the industry in developing appropriate service level agreements on aspects like data quality, API uptimes, and response times. Appropriate enforcement mechanisms should also be considered.
- Lastly, adequate industry consultations should be used to inform regulations and decisions on technology, operational, and business model aspects. The incidence of the costs associated with open banking could be concentrated on the incumbents, while the benefits are more widely dispersed. This calls for active consultations and appropriate mechanisms to ensure incentives are aligned.

Early regulatory efforts have been concentrated on defining standardized API frameworks, creating governance bodies and rules, enhancing security, developing infrastructure, and establishing authentication methods. Among the next items on regulators' agenda in the area of open banking are issues such as the future scope of open banking, competition with other industries, especially with big tech players, and international interoperability.

In that respect, market participants and regulators are starting to talk about the evolution of the scope of open banking toward open finance and smart

data. Open finance refers to the capacity of consumers to access their data via a suite of finance products, including mortgages, savings, insurance, pensions, and so on. On the other hand, smart data suggests the idea of customers accessing their data in nonfinancial services sectors, such as energy, water, mobile, and data from bigtechs. Although the only country to regulate the extension of open banking to other sectors so far is Australia, discussions around it are taking place at different levels in other areas. The idea of reciprocity when giving access to data is a principle that banks are starting to claim as a necessary step toward a level playing field. The Smart Data Review in the United Kingdom and the report of the Canadian Senate Committee on Open Banking also go in the direction of extending access to data to other sectors beyond banking.

Concerning bigtechs, their increasing interest and positioning as financial service providers, especially through banking-as-a-service models, has raised questions about the impact of their access to data from financial institutions. Some banks are starting to claim the idea of reciprocity in the access to customer data to guarantee a level playing field. On the other hand, regulatory authorities are analyzing the implications for financial stability and consumer protection, and also the division of responsibilities between bigtechs and their partnering banks.

Finally, one last element on the agenda of open banking that could contribute to the development of global markets is international interoperability, still at very early stages of discussion. The fact that there is no globally adopted API standard, and that TPPs may need to use different API standards to communicate with banks in different jurisdictions, could lead to potential challenges, such as inefficiencies for third parties or fragmentation of the digital financial ecosystem.