OPEN BANKING: A CASE STUDY IN THE BENEFITS OF INTEROPERABILITY

Alexander Rigby & Chinmayi Sharma*

June 2024

Interoperability and data portability mandates aim to decentralize data governance and increase openness and new technologies like open banking. But relying solely on increased interoperability to combat the issues caused by centralized platforms is unlikely to achieve many of the mandates' stated goals.

The very architecture of the internet is undergoing a profound transformation driven by an increasingly prevalent regulatory trend: interoperability and data portability mandates. Interoperability mandates demand companies build access into their platform services and data stores for third parties, including competitors. Data portability mandates demand companies build mechanisms by which users can access and move their own information from one platform to another. Intrinsic to both regulatory pushes is a concern over centralized platforms retaining outsized influence over both an individual user's online experience and the internet's impact on overall public welfare. Underlying these proposals is an assumption that decentralizing data governance and increasing openness on the internet will foster innovation and competition while empowering and protecting consumers.

The past few years are rife with examples of how centralized platforms prioritize corporate interests over the public welfare. The biggest technology companies get away with poor cybersecurity hygiene, exploitative data practices, disregard for the disparate impact of platform design on marginalized communities, and complicity in the use of platforms by adversaries, domestic and abroad. When Elon Musk took over Twitter, now X, and undid years-long trust and safety policies virtually overnight, many

* Alexander Rigby is law clerk to Chancellor Kathaleen St. Jude McCormick, Delaware Court of Chancery. Chinmayi Sharma is an associate professor at Fordham Law School and former scholar in residence at the Robert Strauss Center for International Security and Law and lecturer at the University of Texas School of Law. We greatly appreciate the help and encouragement of Alan Rozenshtein and the rest of the *Lawfare* team for bringing this paper across the finish line.

users fled the centralized platform to decentralized alternatives like Mastodon and Bluesky.[1] Rather than continue to engage on a platform that saw a near-immediate spike in hate speech and misinformation after the unilateral policy changes,[2] users opted to forego the perks of a well-resourced centralized platform for user-oriented alternatives, which prioritized privacy and user control. Similarly, disillusionment with the way in which centralized platforms cooperate with government surveillance has led to an influx of users joining Signal, an end-to-end encrypted messaging platform built on an open protocol where there is no central authority with access to all user-generated data.[3]

In light of these examples and many more, advocates for interoperability and data portability fear leaving control to the whims of profit-driven entities over internet services that are essential to living a meaningful life socially, politically, and economically. Gatekeeping power over important online functions is borne of exclusive, restrictive control over user data and platform services. So, across nations and industries, there is a growing recognition of the value and necessity of facilitating the seamless exchange of data and services *between* platforms. In the European Union (EU), the General Data Protection Regulation requires platforms to allow individuals to access and transfer their data between service providers, while the revised Payment Services Directive (PSD2) requires banks to allow third-party financial service providers to access financial data and services held by banks.[4] Most notably, the Digital Markets Act's interoperability and data portability mandates took effect in early March 2024, requiring companies identified as "gatekeepers" to open third-party access to their data and services. The United States has also pushed for health care institutions to allow patients to *securely* transfer their highly sensitive health information across health care providers that may use different data management platforms.[5] These are but a few examples of various national interoperability and data portability mandates, responding to the demands of a data-driven era while simultaneously redefining the way we understand and harness the power of information.

---

[1] Alan Z. Rozenshtein, "Moderating the Fediverse: Content Moderation on Distributed Social Media," 3 *Journal of Free Speech Law* 217, 218 (2023) ("The importance of decentralization and open protocols is increasingly recognized within Silicon Valley.").

[2] Sheera Frenkel & Kate Conger, "Hate Speech's Rise on Twitter Is Unprecedented, Researchers Find," *N.Y. Times* (Dec. 2, 2022).

[3] Sasha Lekach, "Signal Hits No. 1 in Apple's App Store After Elon Musk Boost," Mashable (Jan. 11, 2021); Queenie Wong, "Why WhatsApp Users Are Pushing Family Members to Signal," CNET (Feb. 5, 2024).

[4] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 15-20, 2016 O.J. (L 119); Council Directive (EU) 2015/2366, arts. 66-67, 2015 O.J. (L 337).

[5] 45 C.F.R. § 164.524(c)(3) (2014).

In this paper, we argue that relying on increased interoperability to combat the shortcomings of internet centralization is not that simple. Although these regulatory interventions are well intentioned, they are unlikely to achieve their stated goals in isolation. And, more concerningly, they are likely to entrench the very problematic power structures on the internet that they aim to dismantle. In other words, without corollary efforts to break up concentrated marketplaces before introducing robust interoperability and data portability requirements, such mandates will ultimately benefit the existing dominant players.

This argument is borne out in the open banking world—open banking was one of the first regulatory efforts to mandate architectural changes to technology in an effort to decentralize power in the industry. Open banking requires banks to build technological avenues for third-party financial services providers to access financial information and financial service–related functionality. Open banking has seen several victories, for example, by making way for innovative new products that empower consumers, such as Rocket Money. However, it has also met some stumbling blocks: Its potential to decentralize power in the financial industry is stymied by the overwhelming dominance of banks in the space.

Using open banking as a case study, we will first illustrate the harms of allowing internet gatekeepers to amass and exploit outsized amounts of market power. Then we will explain how interventions such as open banking seek to disrupt these power structures and decentralize the industry by changing the very technologies on which it relies. We will highlight why, in isolation, these otherwise commendable measures will at best achieve limited success and at worst exacerbate the underlying problem, by showcasing open banking efforts internationally and at home. Finally, we will recommend that the United States prioritize a proactive approach to decentralization of the finance market as a necessary complement to open banking interventions.

Through this paper, we will ultimately provide a strategy for executing this transition, aiming to enhance opportunities for emerging fintech firms, bolster consumer autonomy and security, and maintain a competitive and democratic system. As the open banking case study will demonstrate, technological changes to the internet cannot, on their own, reshape the power structures that harm consumers and the public today. Before anything else, policymakers need to decentralize decision-making power in industries before true technological decentralization can occur.

FIXING THE GATEKEEPER PROBLEM

The political and economic consequences of centralization and consolidation have been the focus of centuries of scholarship and lawmaking—from Alexis de Tocqueville's *Democracy in America* to the contemporary works of Tim Wu and Lina Khan.[6] In this section, we will review the harms of centralized platforms to essential digital services and the role interoperability can play in addressing the problem.

[6] See, generally, Timothy Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (2018); Lina M. Khan, "Amazon's Antitrust Paradox," 126 *Yale Law Journal* 710 (2017).

Programming Languages

Centralization within the digital domain is a double-edged sword, embodying a complex interplay of efficiencies and monopolistic dangers. On the one hand, the consolidation of control under a few key players—gatekeepers—can streamline operations, simplify oversight, and bolster the reliability of essential services. Yet the very mechanisms that foster these efficiencies also harbor the seeds of overreach. Left unchecked, centralization can empower these dominant entities to box out competition and erode user autonomy, leading to a landscape where innovation is stifled and user interests are subordinated to the whims of the few.

The merits of centralization are not to be overlooked. Gatekeepers, by virtue of their consolidated control, can offer a measure of guarantee against the failure of critical digital services, with more resources and expertise to prevent or mitigate disasters. This centralized authority also enables quicker and more cohesive responses to the evolving needs of the user base, enhancing the overall accessibility and efficiency of digital services. For instance, the streamlined governance of the Domain Name System (DNS), functioning as the internet's directory connecting domain names to IP addresses, ensures that the internet remains navigable and functional, underscoring the practical benefits of having fewer, but more capable, hands at the wheel. Further, gatekeepers can be easier to hold accountable, with fewer players to keep track of and a heightened importance for institutional credibility.[7] The existence of these gatekeepers, by concentrating resources and decision-making, can enhance the accountability of service providers and the adaptability of services to meet changing user demands, promoting a more accessible digital environment.

However, the very benefits of centralization give rise to its shortcomings. Because centralization offers many conveniences, increased demand for centralization can make gatekeeper control over data and user experience absolute, locking them in as the primary, and often only, suppliers of essential digital services. Then, gatekeepers become a problem. With unchecked power, they begin "to diminish the success factors that enable the internet to thrive—scalability to meet the demands of new users, adaptability to encompass new applications, flexibility to enable deployment of new technologies, and resilience to shocks and changes."[8] Generally, these conditions exist when gatekeepers are incentivized to compete for control of the market rather than within the market.[9] The concentration of power among gatekeepers not only poses a risk to the openness and democratic ethos on which the internet was

[7] Nathan Schneider, "Decentralization: An Incomplete Ambition," 12 *Journal of Cultural Economics* 265 (2019).

[8] Michael Kende, Amund Kvalbein, Julia Allford, & David Abecassis, "Study on the Internet's Technical Success Factors," Analysys Mason (December 2021), https://perma.cc/M72P-XKWM.

[9] See generally, Stigler Center for the Study of the Economy and the State, Committee for the Study of Digital Platforms: Market Structure and Antitrust Subcommittee, Draft Report (May 15, 2019), https://perma.cc/EGF7-NPXK.

founded but also exacerbates the issues of market control and user exploitation. This shift away from the internet's foundational principles of openness and accessibility has profound implications, entrenching gatekeeper power and inflicting significant harm on individuals, the private sector, and the public sector alike.

Market centralization engenders the development of internet architectures that are closed, not open. On an open internet, users and producers have equal opportunity to access, interact with, and build within the existing ecosystem. At its purest, this would mean free, open, *infinitely available* space for anyone to build anything without anyone else's permission. In a closed internet landscape, gatekeepers control access to portions of the internet, limiting the availability of content, the creation of new content, and the ability to interact across different types of content. Imagine an alternate universe in which one company or one government owned the internet and required entities to apply and be vetted before allowing them to use it. This is the very risk the founders of the internet fought hard to avoid.[10] Even in the early days of the web, the internet's founders emphasized a need for important services, such as digital identity, property transfer, communication, and finance, to be built democratically and openly.

However, modern times have not seen that vision borne out. While the core of the internet stack—the protocols on which the entire World Wide Web was developed—is still open and permissionless, market centralization has led to walled gardens at the stack's top level, the application layer. Instead of delivering important internet services through open architectures that can interact seamlessly with other internet players, allowing for a more collaborative online environment, platforms have built proprietary fiefdoms aimed at excluding third parties and trapping users in closed ecosystems. These platforms enable companies to amass unprecedented amounts of data about individual users—data that reinforces their power as gatekeepers, which in turn enables them to collect even more data.[11]

Today's gatekeepers were yesterday's startups. These startups flourished *because* the internet was still quite open when they emerged. However, with the newfound dominance they obtained because of openness, these gatekeepers seek to close the door behind them, reshaping the internet into a closed space that precludes the same incubation of new startups that might unsettle their market share.

Closed online platforms and walled gardens, by their very design, severely restrict interoperability, creating ecosystems where data, services, and applications cannot freely interact across different environments. This lack of interoperability significantly undermines user autonomy by locking users into specific platforms and making it difficult to switch services or leverage multiple ecosystems without

[10] Michael Dertouzos & Joel Moses, *The Computer Age: A Twenty Year View* (1980).

[11] Mark Nottingham, "Internet Centralization: What Can Standards Do," mnot blog (March 3, 2023), https://perma.cc/GKT5-WPDQ.

encountering substantial barriers.[12] From a privacy and security standpoint, these closed systems concentrate user data within singular entities, creating lucrative targets for malicious actors and reducing the user's control over their own information. It also incentivizes the unfettered collection of user data because data is the currency of internet dominance today. Moreover, closed platforms restrict innovation by preventing new and emerging technologies from seamlessly integrating with existing services, curtailing the potential for cross-platform innovation and the natural evolution of digital services. When consumer choice is restricted, platforms lack the incentive to rise to a higher standard of care.[13] While centralization may offer benefits in terms of efficiency and streamlined operations, it should not come at the expense of autonomy, privacy, security, and innovation. These values are paramount to maintaining a healthy, vibrant, and competitive digital landscape, ensuring that the internet remains a space for open development, collaboration, and user empowerment.

The Role of Interoperability

Accusations of market centralization are like dog whistles to antitrust advocates. But depending solely on antitrust law to tackle these challenges in finance is misguided. The vigor and direction of enforcement fluctuate with different presidential administrations and political climates, and current antitrust practices concentrate primarily on anticompetitive practices and their effects on consumer welfare—in essence, the impact on price.[14] And then there is the dependence that enforcement has on funding from a volatile Congress.[15] As academics have chronicled,[16] the existing body of antitrust law and jurisprudence imposes a narrow "consumer welfare" lens that overlooks various harms in the digital age,[17] such as concerns over choice, equality, privacy, and security.

---

[12] See Francis Fukuyama, Barak Richman, Ashish Goel, Marietje Schaake, Roberta R. Katz, & Douglas Melamed, "Report of the Working Group on Platform Scale," Stanford Cyber Policy Center (Nov. 17, 2020), https://perma.cc/TG47-UCS5.

[13] Bennett Cyphers & Danny O'Brien, "Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine," Electronic Frontier Foundation (July 24, 2018), https://perma.cc/7T6K-47QZ.

[14] See Frank H. Easterbrook, "The Limits of Antitrust," 63 *Texas Law Review* 1, 1 (1984) ("The goal of antitrust is to perfect the operation of competitive markets.").

[15] See Danielle Kaye, "Biden Requests $63 Million Boost to DOJ's Antitrust Division," Bloomberg Law (March 11, 2024) (noting the "heated debates in Congress over changes to the agency's funding streams").

[16] Timothy Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (2018); Lina M. Khan, "Amazon's Antitrust Paradox," 126 *Yale Law Journal* 710 (2017).

[17] See Richard A. Posner, "Antitrust in the New Economy," 68 *Antitrust Law Journal* 925, 925–26 (2001).

But law is only one of several options in a toolkit of ways to influence technology.[18] There is a growing trend among technologists, policymakers, and civil society calling for changes in the architecture of these walled gardens to combat the harms of centralization. [19] Instead of relying solely on ex post structural antitrust remedies, some observers have proposed introducing more interoperability,[20] through protocols, middleware, and decentralized architectures, as a solution to combat the continued centralization of platform power.[21]

Interoperability broadly refers to the ability of two platforms or products to interact with each other. Without interoperability, a Verizon user would not be able to call an AT&T user in the same country, let alone a Vodafone user overseas. Without data portability, a Verizon user would not be able to port their number over to an AT&T user. Similarly, the global economy rests on the shoulders of the SWIFT banking system, which is a highly interoperable messaging network that banks use to securely transmit information, enabling transactions across numerous different currencies, languages, time zones, regulatory regimes, and technologies.[22] Both forms of interoperability are made possible by the establishment of standardized protocols and are reinforced by collaboratively established policies.

There is a wide range of technological approaches to enabling different types of interaction between platforms, each with its own benefits and shortcomings. Interoperability is not a binary but rather is measured in degrees. Sometimes, interoperability exists only within the firm—when Meta (then Facebook) acquired Instagram, it rebuilt its architecture to allow the company to exchange data between platforms, which gave users the ability to cross-post.[23] However, third-party social media platforms don't benefit from this within-the-firm interoperability—to them the platform is still closed.

To foster true openness, interoperability must exist between different entities. However, even here, there are many ways to accomplish this, each with its own trade-offs. For example, a technological approach

---

[18] Lawrence Lessig, *Code: and Other Laws of CyberSpace* (2022).

[19] Chris Riley, "Unpacking Interoperability in Competition," 5 *Journal of Cyber Policy* 94, 94–95 (2020) ("[T]he future direction of regulatory travel will be towards the promotion of interoperability."); Chinmayi Sharma, "Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability," 50 *University of Memphis Law Review* 441 (2019); Carl Gahnberg, "White Paper: Considerations for Mandating Open Interfaces," Internet Society (December 2020), https://perma.cc/DYB9-7FZF.

[20] Cory Doctorow, "Adversarial Interoperability," Electronic Frontier Foundation (Oct. 2, 2019), https://perma.cc/5P47-8CKB.

[21] See, e.g., Fukuyama et al., supra note 12.

[22] See, e.g., Swift, "Connecting Digital Islands: Swift CBDC Sandbox Project," Results Report (March 2023), https://perma.cc/9PR6-S5VF.

[23] Adam Mosseri & Stan Chudnovsky, "Say Hello to Messenger: Introducing New Messaging Features for Instagram," Meta (Sept. 30, 2020), https://perma.cc/6AG8-JJ47.

to interoperability that gives users the most control over their data may be prohibitively expensive for startups to adopt, undercutting the innovation.[24] Identifying which approach to adopt will depend on the use case and the stated goals: for example, fostering innovation, empowering customers with their own data, or encouraging the adoption of more consumer-protective practices. Adopting the wrong approach risks not only failing to solve the problem but also exacerbating the underlying problematic power structures.[25] Although interoperability can be accomplished through myriad technological means, the dominant approaches include application programming interfaces (APIs), middleware, standard protocols, and decentralized architectures. Each approach comes with its own strengths and weaknesses, which means no one approach is the clear "winner" or universal solution to the problem of centralization. The trade-offs necessitated by each approach must be evaluated on a case-by-case basis—in all likelihood, different technological approaches to interoperability are best suited for introducing openness to different functions.

Early Computing Standards

Perhaps the most commonly referenced approach to interoperability, APIs serve as a crucial conduit for interoperability within the digital ecosystem. They act as a set of rules, protocols, and tools for building software and applications, enabling different digital services and platforms to communicate with each other directly. By defining methods of requesting and exchanging data, APIs facilitate seamless interaction between disparate systems, regardless of their underlying technology. This capability not only enhances the functionality and reach of digital services but also promotes a more integrated and cohesive user experience. Through APIs, platforms can extend their capabilities, allowing external developers to create complementary services, thereby fostering innovation and expansion within the digital landscape.

Increased interoperability through APIs[26] can be accomplished in a few different ways. One option is data portability. The International Organization for Standardization defines "data portability" as the

[24] Miriam Reisman, "EHRs: The Challenge of Making Electronic Data Usable and Interoperable," 44 *Pharmacology & Therapeutics* 572, 574 (2017) ("[T]he financial costs of implementing [electronic health records] remain a primary barrier to their adoption.").

[25] One of interoperability's strongest advocates, Cory Doctorow, writes that while he supports the European Union's push for interoperability, he had "grave concerns about its implementation" because he believed "a hasty interoperability mandate could endanger all kinds of people, everywhere." Cory Doctorow, "An Urgent Year for Interoperability: 2022 in Review," Electronic Frontier Foundation (Dec. 28, 2022), https://perma.cc/QRW3-65Y2.

[26] Data portability can also be accomplished through other technologies, such as web hooks and web sockets, but the dominant technological approach is the use of APIs.

"ability to easily transfer data from one system to another without being required to re-enter data."[27] This can include individual user data, bulk or aggregate user data, metadata or telemetry, as well as insights or inferential data derived from user data. When a gatekeeper allows data to be shifted off the platform, it opens the door into a walled garden and relinquishes exclusive control over that information.

However, not all data portability is made equal. At the very least, APIs can be leveraged by companies to enable consumers or third parties to transfer user data away from their platforms. This data portability can be executed ad hoc—triggered at the user's or third party's request—or programmatically, through regular intervals or live data streaming. Ad hoc data portability, while less complex and demanding on resources for the platform, offers limited utility to users and third parties. It is a highly manual process, and because the information transferred is not standardized, it becomes cumbersome for other platforms to utilize effectively. Additionally, this method does not support multi-homing, the practice of maintaining a presence across multiple platforms simultaneously, due to its sporadic and unstructured nature.

Conversely, programmatic data portability represents a more robust form of interoperability. Also relying on APIs (or web hooks or web sockets, close cousins of the API), this approach allows third parties to access data directly, bypassing the user, which can significantly enhance user control, competitive efficiency, and innovation. Live data streaming, a subset of programmatic portability, ensures real-time data sharing, enriching the dynamism of user interactions across platforms and bolstering autonomy from the dominant platform—for example, financial or health dashboards are not useful unless they reflect moment by moment up-to-date data from other applications.

However, even this model is not without its limitations. Programmatic data portability is less manual in some ways but, like ad hoc data portability, still requires the receiving party to reformat the data received into a standard schema to be able to combine information from one platform with information obtained from another platform. For example, if each bank provided data in a different schema, then a third-party financial dashboard application would need to standardize across those schemas to present a user with a holistic view of their finances. This makes interoperability resource intensive for the third party. Moreover, broadening the category of third parties with access rights, as well as the amount and type of information made available, introduces privacy and security risks particularly if the vetting of these entities is not stringent. Thus, while programmatic data portability advances the goals of interoperability, it necessitates careful consideration of its implications for privacy, security, and resource allocation.

Beyond facilitating data availability, APIs can significantly extend their utility by enabling access to critical functions such as user authentication, payment processing, and content moderation, among others. These functions are fundamental to the operation of digital platforms, ensuring secure user access, facilitating financial transactions and property transfers, and maintaining a safe, secure, and

[27] International Organization for Standardization (ISO), "Automation Systems and Integration—Oil and Gas Interoperability," at 3.23, ISO Standard No. 18101-1:2019 (2019), https://perma.cc/9GKX-ZJSM.

ethical online environment, respectively. Developing these intricate systems from scratch demands a considerable investment of expertise and resources, a requirement that can be prohibitive for smaller competitors or new entrants to the market. The complexity and technical know-how required to implement these features effectively mean that without access to established, reliable APIs, smaller entities might struggle to meet the high standards necessary for such critical operations.

From a privacy and security standpoint, users have reason to distrust third-party providers of these important functions. Dominant platforms, with their established reputations and substantial resources, are generally perceived as more reliable and secure custodians of sensitive user data and functions. By mandating that these platforms make critical functions available through APIs, the digital ecosystem can leverage the trust and security associated with these dominant entities while simultaneously lowering the barriers to entry for competitors. This access allows smaller players to focus their limited resources on developing innovative products and services that complement or enhance the existing offerings rather than expending them on replicating complex foundational services. This hypothesis has real-world support already: The proliferation of Google, Meta, Amazon, and Apple logins and the widespread use of digital wallets show how user authentication can be outsourced to a third party. This form of interoperability can also have privacy benefits, by limiting the amount of sensitive data a user has to turn over to a third-party application. For example, by using an API, a third-party finance app can authenticate whether a user is the client of a particular bank without needing to collect reams of information and process them internally.

While leveraging APIs from dominant platforms to provide core internet functions offers numerous advantages, including lowering barriers to entry and ensuring high-quality services, this approach has significant drawbacks. A primary concern is that it further entrenches the reliance of the digital ecosystem on a few dominant platforms for essential services. This dependence can lead to a form of vendor lock-in, where competitors and users become so integrated with the services of these platforms that switching costs become prohibitively high. Such a dynamic stifles the competitive landscape, potentially leading to less innovation and higher prices over time as dominant platforms leverage their indispensability.

Moreover, by routing critical functions through dominant platforms, an extensive amount of valuable user information is funneled directly to these entities. This situation exacerbates the already considerable data accumulation by these platforms, amplifying concerns regarding data monopolization and privacy. The data collected through services like authentication and payment processing is often highly sensitive, including personal identification details and financial transaction records. When dominant platforms act as the gatekeepers for these services, they gain unprecedented insights into user behaviors, preferences, and social networks, further solidifying their market position and enhancing their ability to monetize user data. This consolidation of data not only raises privacy issues but also reinforces the market power of these platforms, as the data they collect can be used to refine their algorithms, tailor their services, and potentially exclude or undermine competitors.

Middleware

To alleviate the burden on smaller competitors of translating across different APIs, the market can foster a derivative industry of middleware software. Middleware acts as a crucial intermediary layer that standardizes and translates data automatically across different APIs, providing end users with combined data in a single, standard schema. This technology functions by connecting disparate systems and protocols, effectively bridging the gap between different platforms' unique APIs and data formats. With middleware, the process of integrating and utilizing data from dominant platforms becomes significantly more streamlined for users and competitors. This automation reduces the manual effort required to align with each platform's specific requirements, thereby lowering the barriers to access and use of data across the digital ecosystem.

The primary advantage of middleware lies in its capacity to enhance operational efficiency and interoperability, facilitating smoother interactions and data exchange between platforms with minimal user intervention. A prime example is MuleSoft's Anypoint Platform, an enterprise-level middleware that enables companies to integrate diverse systems, applications, and data sources. Anypoint offers components like connectors, APIs, and data mapping tools for connecting disparate systems and transforming data into a common format, along with administrative tools for managing integration, security, and platform governance. However, the effectiveness of middleware is inherently contingent on the dominant platforms' willingness to make their data accessible, including the timing, extent, and manner of data availability. Its functionality is highly sensitive to changes in the platforms' APIs; any modification can disrupt the middleware's operation until it is updated to accommodate the new changes. This dynamic introduces a significant rigidity into the system, as the middleware must adapt constantly to keep pace with evolving platform standards.

Moreover, the responsibility of developing and maintaining middleware falls on third parties, which often means smaller entities bear the burden of ensuring compatibility and functionality across different systems. This arrangement places a disproportionate amount of pressure on these third parties, rather than on the dominant platforms, which would be more capable of facilitating interoperability through the adoption of standardized data formats. By requiring dominant platforms to standardize their APIs and data schemas, the burden of achieving interoperability would shift to the "least cost avoider"—the entity most able to effect change at the lowest relative cost. Such an approach would not only level the playing field but also promote a more open, accessible, and competitive digital landscape, aligning with the broader goals of innovation and user empowerment.

Standard Protocols

An alternative to the API-centric model that reduces reliance on dominant platforms and mitigates the risk of entrenching their market power involves the development and utilization of standard protocols.[28] Standard protocols are platform-neutral agreed-upon sets of rules and formats for data exchange and communication across the internet, designed to ensure seamless interoperability between different systems and platforms. Examples of these protocols include the Hypertext Transfer Protocol (HTTP) for web communication, the Simple Mail Transfer Protocol (SMTP) for email transmission, and the Internet Protocol (IP) itself, which underpins all internet traffic.

These protocols are typically developed in open, transparent processes by international bodies like the Internet Engineering Task Force (IETF), which operates independently of any single company or country's interests.[29] The IETF, among other independent standard bodies, fosters a collaborative environment in which experts from around the globe contribute to the design and improvement of protocols, ensuring they are crafted in a user-centric manner. This approach to standardization promotes a foundational level of interoperability across the internet, enabling technologies and services to communicate and function together without proprietary barriers. It embodies a true form of openness, where the permissionless use of these protocols facilitates innovation and competition.

The adoption of standard protocols offers several advantages, including reducing the digital ecosystem's dependency on any single platform's infrastructure for essential internet functions. This fosters a more competitive environment in which new entrants have a fairer chance to innovate and thrive. Additionally, it aligns with the original vision of the internet as an open platform for communication and collaboration, free from the control of gatekeeping entities. Indeed, the existence of an open internet stack is credited with the proliferation of innovation in the early days of the internet, when entities were able to explore and experiment with the new technology without any gatekeepers prohibiting access or the need to coordinate across different proprietary architectures. By utilizing established protocols, developers and organizations can avoid the costly and redundant process of creating proprietary systems for basic interoperability.

However, this approach is far from a silver-bullet solution. One challenge is the pace of development and adoption; the consensus-driven process of standard-setting bodies can be slow, potentially lagging behind the rapid innovation cycles of the technology industry. Additionally, while standard protocols level the playing field in theory, in practice the implementation and extension of these protocols by dominant platforms can still lead to variations that subtly favor their services. Moreover, achieving widespread adoption of new or updated standards across the entirety of the internet's sprawling and decentralized architecture can be a daunting task, requiring significant coordination and cooperation

[28] Chris Riley, "A Framework for Forward-Looking Tech Competition Policy," Mozilla Working Paper (Sept. 9, 2019), https://perma.cc/PLU3-VZPR.

[29] Internet Engineering Task Force, "Introduction to the IETF," https://perma.cc/76WG-9XC8.

among a diverse array of stakeholders. Despite these challenges, the development and use of standard protocols remains a crucial strategy for preserving the internet's openness and ensuring its continued evolution as a platform for innovation and access.

Decentralized Architectures

Finally, some interoperability solutions are best characterized as decentralized. In this paper, we use the term "decentralized architecture" to refer to the technical concept of disaggregating decision-making in a network.

Blockchain is one form of decentralized architecture. It is a distributed ledger technology that records transactions across multiple computers in a manner that ensures the integrity and security of the data without the need for a central authority. Each participant in the network has access to the entire database and its complete history. No single participant controls the data or the information, which promotes democratic control over the network and avoids gatekeeper rule by fiat. Every transaction is verified by the consensus of a majority of the participants in the system. This decentralization ensures that the system is transparent, secure, and resistant to censorship.

In terms of interoperability, blockchain can facilitate seamless transactions and interactions across different platforms and systems without the need for intermediaries. This could include the transfer of digital assets, identities, or even data across disparate platforms with trust and security baked into the protocol. However, blockchain technologies face challenges such as scalability, energy consumption, and the complexity of integrating with existing systems. Additionally, the fragmented nature of blockchain ecosystems can sometimes hinder interoperability rather than enhance it, unless specific protocols or standards are adopted network wide.

Federated environments, by contrast, operate through a model of connected yet autonomous nodes or servers, allowing individual platforms or services to communicate and share data under a common set of standards without central control. This model is often seen in communication platforms (like email or instant messaging), or social media networks, such as Mastodon, where users on different servers or in different network instances can interact seamlessly. For example, in Mastodon, users can establish their own instance of the social network, customized to reflect their own preferences for content moderation and privacy, while still ensuring interoperability with other Mastodon network instances.

Federated models promote interoperability by allowing diverse systems to connect and operate together, maintaining their independence while sharing certain functionalities. This approach is particularly advantageous for preserving user autonomy and preventing data monopolization, as it avoids the concentration of power and information within a single entity. No one can be fully excluded from the "fediverse," the overarching ecosystem of federated technologies. However, it is limited by network effects, in that users are hesitant to switch over to federated alternatives to dominant platforms.

None of these technological approaches, from ad hoc data portability to decentralized architectures, can achieve every goal of interoperability to the same degree at the same time. Increased interoperability

"does not automatically yield an egalitarian, equitable or just social, economic, political landscape."[30] Determining which technological approach to use for a specific problem must begin with an analysis of what the goals are *for the specific context in which interoperability is being evaluated as a possible solution.* And then, for any of these to work, they need to be augmented with proactive measures to deconsolidate the market in addition to decentralizing the architecture.

THE PROMISE OF OPEN BANKING

The case study of open banking is illustrative of both the importance of identifying the *right* technological approach to interoperability to serve each use case as well as the fact that interoperability mandates, on their own, won't achieve the stated goals of user empowerment and improvements in social welfare, without other regulatory efforts to deconsolidate the banking industry.

Open banking, by design, mandates that banks provide third-party providers access to consumer financial data through APIs, aiming to foster innovation, competition, and user empowerment. Under most regulations internationally, open banks must provide certain third parties dedicated APIs for account, payment, and authentication services as well as access to consumer banking data,[31] though some countries, such as India, are moving toward government-controlled digital payment protocols.[32] In a banking world that has grown increasingly centralized, the open banking movement presents a beacon of hope. Indeed, 2022 and 2023 were the years open banking gained worldwide prominence,[33] and, due to regulatory interventions, the open banking market is expected to soar to a projected value of U203.8 billion by 2033, with a projected compound annual growth rate of 23.3 percent from 2024 to 2033.[34]

But when a financial market is dominated by a few players, interoperability mandates risk being undermined as these dominant entities can exert significant influence over the shaping of interoperability policy and the selection of interoperability solutions. Given their substantial market power and vested interests, these players are likely to favor solutions that align with their own strategic

---

[30] Balázs Bodó, Jaya Klara Brekke, & Jaap-Henk Hoepman, "Decentralisation: A Multidisciplinary Perspective," 10 *Internet Policy Review*, no. 2 (June 2021).

[31] European Central Bank, "The Revised Payment Services Directive (PSD2) and the Transition to Strong Payments Security" (March 2018), https://perma.cc/HG2F-L3W5.

[32] Yan Carrière-Swallow, Vikram Hanksar, & Mansa Patnam, "Stacking Up Financial Inclusion Gains in India," International Monetary Fund (July 2021), https://perma.cc/DD9W-B5G9.

[33] Steve Cocheo, "Why Open Banking Is a Must-Have for U.S. Financial Institutions," The Financial Brand (Feb. 6, 2023), https://perma.cc/9KXS-GPUU; Simone Martinelli, "2023 Will See the Start of Consumerization in Open Banking," Nasdaq (Jan. 9, 2023), https://perma.cc/GNT3-KV52.

[34] Market.Us, "Open Banking Market to Soar to USD 203.8 Billion by 2033 | Driven by Digital Transformation and Regulatory Initiatives," Yahoo Finance (Feb. 15, 2024).

objectives, potentially at the expense of broader market competition and innovation. Consequently, without careful regulation and oversight, the intended benefits of interoperability, such as increased consumer choice and enhanced service innovation, may not fully materialize, as the solutions adopted may serve primarily to reinforce the status quo rather than challenge it. The biggest threat to the success of open banking is the root of the problem itself: the consolidated banking industry.

Consolidation of the Banking Industry

Over the past twenty years, the American financial system has become more and more consolidated. This is the result of both policy and the 2008 financial crisis, which allowed surviving financial institutions to "scoop up" those that had failed.[35] Today, the five biggest commercial banks in the United States make up nearly half of the system's assets—J.P. Morgan Chase and Bank of America, which together control just under 35 percent of the market.[36] The number of banks has fallen sharply, and concentration—both locally and nationally—is at unprecedented levels.[37] This process has been described as the "Great Consolidation"[38] and, on the brick-and-mortar level, has depleted local branches, credit unions, and local economic activity.[39] This consolidation is not just horizontal (between banks) but also vertical: Banks are purchasing financial services and technology companies (fintech) with increasing speed.[40] This centralization poses risks: diminished product quality, higher barriers to entry, and increased systemic dangers.[41]

Consolidation has made banks "closed" in two ways—closed to competitors structurally and technologically. First, consolidation has led to exclusionary conduct that keeps competitors out of the market structurally—exploiting their market dominance to raise barriers to entry and take advantage of

---

[35] Jeremy C. Kress, "Reviving Bank Antitrust," 72 *Duke Law Journal* 519, 550–51 (2022).

[36] See generally, Kress, supra note 35; Adam McCann, "Market Share of U.S. Banks by Domestic Deposits," WalletHub (Feb. 26, 2024), https://perma.cc/MKK3-DAU9 (noting that based on 2023 domestic deposits, J.P Morgan Chase and Bank of America had 16.19 percent and 14.78 percent market shares, respectively; based on total assets, they had 19.46 percent and 14.56 percent market shares, respectively).

[37] Kress, supra note 35.

[38] Jad Edlebi, Bruce C. Mitchell, & Jason Richardson, "The Great Consolidation of Banks and Acceleration of Branch Closures Across America: Branch Closure Rate Doubled During the Pandemic," National Community Reinvestment Coalition (February 2022), https://perma.cc/TG2Q-4DE4.

[39] Hannah M. Dunway, "'Breaking the Bank' Mergers: How Bank Consolidation Is Hurting Communities," 27 North Carolina Banking Institute 108 (2023).

[40] Sophia Furber & Gaby Villaluz, "Fintech M&A Deal Tracker: Banks Regain Appetite for Buying Fintechs," S&P Global Market Intelligence (Nov. 17, 2022), https://perma.cc/QB3Q-XWLW.

[41] Kress, supra note 35.

dependent third parties.[42] The ability to box out competitors is augmented by the network effects of exclusive data access—more user data means more tailored platforms, which results in more opportunity to collect data.[43] For instance, a bank with exclusive access to purchasing histories can design cards that reward spending trends and then give customers personalized recommendations for cards that best complement their spending habits. Without the same information, a competitor financial institution has no ability to customize rewards programs to reflect real-time spending patterns nor target advertisements for their credit offerings in the same way, disadvantaging them competitively.

As consolidated firms earn oligopoly rents and benefit from the ability to exclude competitors, they can further close out the finance ecosystem by purchasing fintech companies and their technology before that technology can disrupt the banking system—as is happening daily.[44] While mergers are not per se problematic, too much vertical industry consolidation should be of concern to consumers because it could lead to reduced quality of service up and down the finance vertical.[45] Banks controlling the direct deposits, savings, investments, mortgages, loans, payments, credit management, and more affords them a huge amount of power and locks customers in, reducing the banks' incentive to provide better services since they can keep customers even while offering non-optimal products.[46]

Second, the banking system has been "closed" technologically. Dominant platforms in the financial sector can effectively close off their technologies to third parties by either not offering APIs or, when they do offer them, imposing stringent restrictions on their use. By withholding APIs, these platforms prevent third-party developers and fintech companies from accessing valuable data and functionalities, essential for creating complementary or competitive services. Even when APIs are provided, these platforms may implement restrictive licensing agreements, high fees, or technical limitations that severely constrain the scope of what third parties can do with the data. These restrictions can include limiting the frequency of data access, the types of data available, or the specific functionalities that can be integrated. This approach not only stifles innovation by hindering the development of new and potentially competing services but also consolidates the market power of these dominant platforms by maintaining control over who can enter the market and under what conditions. The result is a less

---

[42] For an example in banking and credit, see *In re* Payment Card Interchange Fee & Merch. Disc. Antitrust Litig., No. 05-MD-1720 (MKB) (JO), 2019 WL 13213700, 2019 U.S. Dist. LEXIS 217583 (E.D.N.Y. Dec. 16, 2019) (approving settlement to a class action alleging that banks harmed competition and charged the merchants supercompetitive fees by creating unlawful contracts).

[43] Steven C. Salop, "Dominant Digital Platforms: Is Antitrust Up to the Task?" 130 *Yale Law Journal Forum* 563, 566 (2021).

[44] See, e.g., Marry Ann Azevedo, "So Much Fintech M&A," TechCrunch (Jan. 15, 2023).

[45] Steven C. Salop, "Invigorating Vertical Merger Enforcement," 127 *Yale Law Journal* 1962, 1975 (2018).

[46] Kress, supra note 35 at 576.

competitive market landscape where third-party access is curtailed, and consumer choice is diminished, ultimately slowing the pace of innovation and progress within the financial sector.

The lack of interoperability and the existence of gatekeepers within the financial sector are particularly concerning due to the critical nature of financial services and the profound impact they have on both individual livelihoods and the global economy. In a sector where transactions, access to credit, and financial information flow are foundational to economic activity, gatekeepers can exert considerable control over what services are available, to whom, and at what cost. This control can lead to a concentration of power among a few dominant entities, stifling innovation, reducing competition, and potentially leading to higher costs for consumers. Moreover, the financial sector's reliance on outdated infrastructure and the prevalence of siloed systems significantly hampers the efficiency and accessibility of financial services. This lack of interoperability not only impedes the seamless exchange of financial information across different platforms and institutions but also limits the ability of consumers to access a broader range of financial products and services. Additionally, in an increasingly digital world, the ability to securely and efficiently move financial data is paramount; thus, any barriers to interoperability can also heighten security risks and undermine trust in the financial system. Given the sector's importance to economic empowerment and the potential for financial technology to drive inclusive growth, overcoming these challenges and ensuring a more open, competitive, and interoperable financial landscape is imperative.

Competition as a Boon to Consumers

On the other side of the marketplace are fintech firms—the third parties seeking increased interoperability. Fintech firms have emerged as pivotal third-party players in the financial sector, primarily in response to the growing demand for more accessible, efficient, and user-friendly financial services. These firms leverage cutting-edge technology to offer a wide range of services, including mobile payments, peer-to-peer lending, personal financial management, and cryptocurrency transactions. Their rise stems from the recognition of gaps and inefficiencies in traditional banking services, such as high fees, slow transaction times, lack of customization, and poor user experiences. By utilizing advanced technologies like blockchain, artificial intelligence, and data analytics, fintech firms are able to offer innovative solutions that are often more tailored, cost effective, and convenient than those provided by traditional banks. They help consumers by democratizing access to financial services, providing greater transparency, enhancing security, and promoting financial inclusion for underserved or unbanked populations.[47] In essence, fintech firms are redefining the financial landscape by introducing more competitive alternatives to conventional banking, focusing on consumer needs and preferences that traditional institutions have been either unable or unwilling to meet.

Fintech firms, despite their innovative edge and consumer-centric models, are concerningly dependent on interoperability with banks to deliver their services in a meaningful and safe manner. For instance,

[47] See Cesare Fracassi & William Magnuson, "Data Autonomy," 74 *Vanderbilt Law Review* 327, 339 (2021).

fintech services like peer-to-peer payments, personal finance management, and digital wallets rely fundamentally on secure access to users' banking information and the ability to initiate transactions on their behalf. This requires cooperation from banks in terms of functions such as authentication, to verify the identity of users securely, and money transfer protocols, to facilitate the movement of funds between accounts within and across different financial institutions. Additionally, services that offer financial advice or investment management need detailed data about consumers' financial transactions and accounts to provide personalized recommendations.[48] Without access to this data and the underlying banking functionalities, fintech firms would be unable to execute these services accurately, securely, and efficiently, significantly limiting their ability to improve consumer experiences and offer innovative financial solutions.[49]

For example, Rocket Money, a prominent fintech company, offers a comprehensive personal financial management solution by aggregating various financial accounts from banks, credit cards, loans, and investments into a single, user-friendly interface, providing consumers with a holistic view of their financial situation as well as tools to decrease their expenditure on subscriptions and utilities. It assists users in budgeting, expense tracking, and achieving their financial goals by analyzing their spending patterns, offering personalized saving tips, and reminding them of upcoming bills. Studies have shown that access to this holistic, real-time view of financial information decreases consumer debt by, among other things, helping users to avoid overdraft fees.[50]

Sadly, fintech firms have been unable to truly disrupt the existing banking architecture. Banks are typically not incentivized to cooperate with fintech firms or facilitate their growth, as fintech solutions often compete directly with their own services, offering more innovative, efficient, and user-friendly alternatives. This competition threatens to erode the customer base and profit margins of traditional banks, providing them with a clear disincentive to support the fintech sector.[51] As a result, some banks resort to contractually and technologically blocking fintech firms' access to consumer financial data, which is crucial for the operation of many fintech services. Giving away the key to the castle undermines the position of each of the big players by making the marketplace more competitive, which should lead to lower prices and a redistribution of incumbent power. None of the current big banks would be inclined to engage in such an endeavor—throwing away oligopoly rents—unless forced to by market pressure, regulation, or, by some miracle, altruism. If companies can sink innovative competitors, then there's no need to invest in making service changes themselves. If they can't, then

[48] Id.

[49] Id.

[50] Bruce Carlin, Arna Olafsson, & Michaela Pagel, "FinTech and Consumer Financial Well-Being in the Information Age," FDIC (January 2019), https://perma.cc/8Z7Y-WG32.

[51] Fracassi & Magnuson, supra note 47.

they can mimic the technologies competitors develop and slowly choke them out of the marketplace by denying them the data they hoard.[52]

Without this access, fintech firms are compelled to use less reliable, less secure, and more invasive methods to gather financial information, such as screen scraping—a process in which a fintech app logs into a bank's online banking interface as the user and copies (or "scrapes") the displayed information.[53] Screen scraping is not a recent development. As far back as 2001, regulators identified the practice of sharing consumer login credentials for data aggregation services as raising additional risks.[54] This practice is not only limited and cumbersome but also increases the risk of fraud and prevents banks from knowing when third parties access data. Fintech companies agree this is not a good solution—but it is the only option available to them in serving customer needs in a closed banking environment. Other unsafe tactics may include using unverified or less secure data sources, such as public open-source information, information purchased from data brokers, or user-provided financial information that may be outdated or inaccurate. These approaches not only compromise consumer security and privacy but also diminish the quality and reliability of the fintech services offered, making them less appealing and, more importantly, less useful to potential users.

Despite a genuine consumer demand for the innovative services provided by fintech firms,[55] these companies often lack the market power to challenge the entrenched position of traditional banks effectively. Without the ability to access necessary financial data directly and securely, fintech firms struggle to scale, compete, and ultimately achieve profitability. Consequently, acquisition by larger financial institutions or tech companies becomes one of the few viable options for fintech startups seeking to sustain their operations. We are already seeing this play out. Since 2021, J.P. Morgan Chase has bought or invested in over 40 fintech firms.[56] This trend not only limits the disruptive potential of fintech innovations but also serves traditional banks by eliminating competitors and potentially

---

[52] See Stulz, "FinTech, BigTech, and the Future of Banks," 31 *Journal of Applied Corporate Finance*, no. 4, at 86–97 (2019); Inna Romanova & Marina Kudinska, "Banking and FinTech: A Challenge or Opportunity?" *Contemporary Issues in Finance: Current Challenges From Across Europe* (2016).

[53] Carlin, Olafsson, & Pagel, supra note 50 at 23, 25, 26.

[54] See Office of the Comptroller of the Currency, "Bank-Provided Account Aggregation Services," OCC Bulletin 2001-12 (Feb. 28. 2001); Federal Financial Institutions Examination Council, *E-Banking*, IT Examination Handbook (August 2003), at App. D.

[55] European Commission, "Payment Services—Review of EU Rules, Public Consultation" (Dec. 15, 2021), https://perma.cc/9VT6-M6VR.

[56] Luisa Beltran, "JPMorgan Chase's FinTech Buying Spree," Yahoo Finance (April 25, 2023), https://perma.cc/E84L-HLAX.

consolidating their market power further, ultimately restricting consumer choice and stifling innovation in the financial services sector.

The acquisition or shutdown of fintech companies by traditional banks tends to be detrimental to consumers for several reasons, particularly concerning privacy, security, quality of service, innovation, and transparency. Fintech firms often introduce cutting-edge technologies and methodologies that prioritize user experience and data security, offering services that are not only more user-friendly but also more secure against cyber threats. For example, Ripple, a blockchain solution, is inherently decentralized, meaning it does not rely on a central point of control that could be a potential vulnerability for attacks or breaches. It also employs advanced cryptography to secure transactions and protect user data, improving privacy and making the ledger resistant to fraud. These new services, developed outside the traditional banking framework, frequently embody a level of innovation and customization that traditional banks have historically been slow to adopt, in part because they are not driven by competitive pressures to do so.

The presence of third-party services generally fosters a healthy competitive environment that naturally drives improvements in service quality across the board. Competition compels all players to continuously enhance their offerings and customer experience. Without this competitive pressure, as is the case in today's consolidated marketplace and would be even more so if traditional banks continue acquiring fintech competitors, banks might opt not to introduce beneficial services or could choose to offer them at a lower quality. They could also impose restrictive or exploitative terms on consumers, knowing that in the absence of alternatives, consumers would have little choice but to accept them. This scenario exacerbates the problem of consumer lock-in, where switching costs become prohibitively high, thereby raising barriers to entry for potential new entrants and stifling innovation. Additionally, with fewer competitors in the market, traditional banks can accumulate and leverage user data in ways that may not align with consumer interests, such as for targeted marketing or differential pricing strategies that could disadvantage certain groups of consumers.

While fintech firms have significantly disrupted the traditional banking sector by offering innovative and consumer-friendly financial services, it's important to acknowledge that not all fintech firms operate with the same level of integrity or competence. Some may engage in shady or unethical practices, lack the necessary competency, or not have sufficient resources to ensure the fair and secure provision of services. These drawbacks, however, are part and parcel of a vibrant, competitive landscape, which is fundamentally considered beneficial and desirable from an economic and legal perspective.

Protecting the public against these concerns is the purview of the government, not of the private sector. Financial consumer protection regulations and privacy laws are designed to mitigate the risks of newer, untested startups or otherwise suspicious players by holding financial service providers accountable and ensuring that they adhere to standards that protect consumer rights and data security. In the United States, for instance, the Consumer Financial Protection Bureau (CFPB) actively monitors and regulates

activities in the financial sector to prevent unfair, deceptive, or abusive practices.[57] Similarly, the Securities and Exchange Commission oversees securities markets and protects investors from fraudulent activities, including those that may involve fintech companies offering investment services.[58] These regulatory bodies have the authority to enforce compliance, conduct investigations, and impose penalties on entities that violate consumer protection laws or securities regulations. For example, the CFPB has taken actions against fintech companies for practices that misled consumers about product benefits or failed to safeguard personal financial data adequately.[59]

Such regulatory actions underscore the principle that while risks are inherent in a competitive landscape, there are established mechanisms in place to address these issues. The responsibility to mitigate risks associated with fintech firms and protect the public interest lies with regulators, not with the private sector. Private entities, driven by self-interest, cannot be expected to prioritize public welfare in the absence of regulatory oversight. Thus, the role of regulators is not only to protect consumers but also to ensure that the competitive landscape remains healthy, diverse, and conducive to innovation, all while safeguarding against the potential drawbacks of a rapidly evolving financial services sector.

The Rise of Open Banking

In response to these realities, international regulators have passed open banking laws demanding more interoperability in the industry. Open banking refers to a banking practice where banks provide third-party financial service providers access to consumer banking, transaction, and other financial data from banks and nonbank financial institutions through the use of APIs or open protocols. The policy principles underlying open banking center on increasing transparency for consumers, fostering competition, and promoting the development of new, innovative financial services that can cater to diverse consumer needs more effectively. A key aspect of open banking is the unbundling of services. This concept involves breaking down traditional banking services into their component parts, allowing third-party providers to offer individual services, such as payment processing or financial management tools, directly to consumers. This unbundling enables consumers to mix and match services from various providers to suit their unique financial needs, enhancing choice and personalization in the financial services market.

---

[57] Sidley Austin LLP, "Recent Analysis of Consumer Financial Protection Bureau Data Shows Exponential Increase in Fintech and Crypto Complaints to CFPB" (July 6, 2021), https://perma.cc/2LAH-XJ3U.

[58] Securities & Exchange Commission, "SEC Charges FinTech Investment Adviser Titan for Misrepresenting Hypothetical Performance of Investments and Other Violation," Press Release 2023-153 (Aug. 21, 2023), https://perma.cc/5NVB-YX86.

[59] Consumer Financial Protection Bureau, "CFPB Issues Guidance to Rein in Rigged Comparison-Shopping Results for Credit Cards and Other Financial Products," Press Release (Feb. 29, 2014), https://perma.cc/AJ6A-R6S8.

Open banking is both a policy and a set of technologies. On the policy side, it is a spectrum of goals. At a base level, it is intended to increase competition in the financial service sector while also granting consumers more data autonomy. The ideal manifestation of open banking principles would be creating a landscape where new entrants compete on *equal footing* as existing players, creating virtual banks that operate on existing banking infrastructure. The four foundational *policy* principles of open banking are (1) data access—the customer's ability to view the entire range of information an institution has on them; (2) data sharing—giving customers the power to allow third parties to transact on their behalf; (3) data portability—the ability to easily transfer data from one platform to another; and (4) data interoperability—the ability of two or more systems to exchange information.[60] Policies are focused on unbundling and disrupting vertical integration between banks and other service providers (like fintech) to allow new entrants to offer alternatives to different links in the value chain. Different countries are going about this task in different ways, but, at a minimum, open banking regulations push for a liberalization of consumer financial data and the opening of the door to certain banking and finance APIs.

On the technology side, open banking can be accomplished in a variety of ways, each with its own benefits and shortcomings. The EU found that APIs were the most reliable and tested technology to enable the widespread and secure access to user data and are at the core of their open banking regime.[61] The EU's approach to open banking is one of the most structured and regulated in the world, mandating that European banks must be "open" under the revised Payment Services Directive. PSD2 requires all banks in member states to provide certain third parties dedicated, *standardized* APIs for account, payment, and authentication services as well as access to consumer banking data. These APIs are established collaboratively and must be common across institutions. It requires that third parties obtain licenses, which mitigates the concern that irresponsible entities can gain access to sensitive customer data. By the end of 2021, the EU gave approval to 529 third-party providers.[62] This regulatory-driven approach ensures a high level of standardization and security across the board, promoting innovation and competition. However, one criticism is that its prescriptive nature may limit flexibility, as it requires banks and third parties to adhere strictly to the defined standards without room for adaptation to specific business models or innovative practices that fall outside these standards.

By contrast, India opted to build a suite of open finance protocols—an approach that, while it has its own trade-offs, provides the most liberalization of the market, by making the technological foundation

[60] Dan Awrey & Joshua Macey, "The Promise & Perils of Open Finance," 40 *Yale Journal on Regulation* 1, 6 (2023).

[61] See Markos Zachariadis & Pinar Ozcan, "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking," SWIFT Institution, Working Paper No. 2016-001, at 10–12 (2017), https://perma.cc/R79N-XA5C.

[62] Mastercard, "Q4 2021 Open Banking Tracker," https://b2b.mastercard.com/newsandinsights/openbankingtracker/q42021/.

of interoperability standard across all players in a market, as opposed to having each company establish its own APIs. India's open banking initiative is premised on a digital identity solution introduced in 2010 with the launch of a biometric digital ID system dubbed Aadhaar—these IDs allow for a single source of truth for identification, streamlining authentication and identity verification for financial institutions. Almost 90 percent of the population signed up for a digital ID in the ensuing decade, with half linking their ID to their bank account. The open banking protocol, governed by the Unified Payments Interface (UPI) under the guidance of the National Payments Corporation of India (NPCI), is a unique public-private partnership. The standard protocol allowed fintech firms and banks to exchange messages and payments seamlessly with any other entity that uses the same UPI protocols—which means users can link multiple bank accounts into a single mobile application, merging several banking features, seamless fund routing, and merchant payments into one platform. Today, street vendors who previously did not have bank accounts can receive payments for goods or services through digital wallets. Fintech firms can expand their offerings and reach the entire country's population if they build off the UPI.[63] This approach emphasizes inclusivity and interoperability across banks and third parties, facilitating a rapid increase in digital payments across the country. While this model has significantly boosted financial inclusion and payment efficiencies, its centralized nature raises concerns over system resilience and the concentration of data control within a single entity (NPCI), potentially creating a single point of failure or data privacy concerns.

The United States is gradually moving toward open banking through a combination of regulatory guidance and market-driven initiatives rather than through a single, comprehensive legislative framework akin to the U.K.'s approach or the EU's PSD2. The Consumer Financial Protection Bureau has been instrumental in pushing for increased data sharing and consumer access rights, laying the groundwork for open banking principles. In October 2023, the CFPB proposed a rule, the Personal Financial Data Rights Rule, that would accelerate the shift toward open banking.[64] This rule provides consumers with agency by granting them authority to revoke access to their own data and obtain their data free of charge.[65] In theory, these developments are poised to benefit consumers by fostering innovation, enhancing financial services, and promoting competition.

However, the U.S. banking sector's highly concentrated nature poses significant challenges to realizing open banking's full potential. Traditional banks, with their established market dominance, might find ways to comply with open banking regulations while still limiting the effectiveness of new entrants. For instance, they could set restrictive terms for API access or offer a less efficient, more cumbersome data sharing process that technically meets regulatory requirements but practically discourages third-party

[63] Yan Carriere-Swallow, Vikram Hanksar, & Mansa Patnam, "Stacking Up Financial Inclusion Gains in India," International Monetary Fund (July 2021), https://perma.cc/DD9W-B5G9.

[64] Consumer Financial Protection Bureau, "CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking," Press Release (Oct. 19, 2023), https://perma.cc/C4JH-S84R.

[65] Id.

providers. Additionally, while open banking aims to level the playing field, the existing dominance of major banks could enable them to leverage newly accessible data to fortify their positions further, potentially even developing or acquiring fintech services that directly compete with smaller innovators. This scenario could lead to a situation in which traditional banks not only retain their market power but also exploit open banking initiatives to entrench their positions further, ultimately undermining the goals of increased competition and innovation.

The Benefits and Shortcomings of Open Banking

Before delving into the regulatory interventions necessary to ensure the success of open banking in the United States, we will first review the benefits and shortcomings of open banking across various equities. It is important to recognize that interoperability is not a monolith or an unqualified good. While it brings significant advantages, such as enhanced competition, innovation, and consumer choice, it also presents challenges, including privacy concerns, potential security vulnerabilities, and the risk of market dominance by a few large players. Recognizing these trade-offs is fundamental because it highlights the inherent tension between multiple goals or values that are important to stakeholders within the financial ecosystem. These goals, such as consumer protection, market efficiency, and data security, cannot all be maximized to the same degree simultaneously. This recognition sets the stage for a more informed discussion of the kind of regulatory framework that can best balance these competing interests, thereby making open banking and interoperability genuinely successful and beneficial for all parties involved.

User Experience

Open banking catalyzes the creation of financial products that are significantly more useful to consumers, primarily by enhancing user experiences through intuitiveness, transparency, and ease of use. This improvement occurs both because fintech companies will directly prioritize user-centric design and innovative functionalities, and because the presence of these new entrants instigates a competitive environment that compels traditional banks to elevate the user experience of their services. For instance, personal finance management apps developed under open banking can aggregate all of a user's financial data across different institutions into a single interface, offering a comprehensive view of their financial health. This not only simplifies the user's experience but also provides actionable insights tailored to their financial behavior, such as budgeting advice or personalized savings goals. Banks are unlikely to provide the same services on their own because they profit from things like overdraft fees or revolving debt.

Increased interoperability can also improve access to financial services or the financial industry entirely. Limiting financial inclusion to the parameters of traditional banks leaves countless individuals out of these essential services. Traditional banks rely on traditional data sources that, when used exclusively, may preclude individuals from important financial tools such as loans. Open banking diversifies the available data and can provide individuals who have thin files or no formal credit histories access to credit. For example, researchers found that including utility data allowed 20 percent of customers with

otherwise threadbare formal financial histories to become "thick-file" customers better able to access financial services.[66]

Improving usability is particularly beneficial for consumers as it fosters a deeper understanding of financial products and services. When consumers can easily navigate their financial interfaces and understand the options available to them, they are better equipped to make informed decisions that align with their financial goals. This enhanced decision-making capacity can lead to more responsible financial management and greater financial well-being over time.

However, this landscape is not without its concerns. As fintech companies rush to fill gaps in the market and respond to consumer demand, there's a risk that some may offer products that claim to provide valuable services but are actually misleading or primarily serve the company's interests. For example, a fintech app might offer an investment platform that promises high returns with low risk but in reality obscures the true risk involved or the fees associated with the service. Or, it might claim to offer a product comparison tool when in reality it drives customers to specific products that would earn the fintech company kickbacks from the manufacturer. Moreover, improved user access and the ease of using financial services can lead to consumers making hasty decisions without fully understanding the long-term implications, such as taking on credit or investments that do not suit their risk profile.

Therefore, while open banking has the potential to significantly improve financial products and user experiences, it also necessitates a cautious approach. Consumers need to be equipped with the knowledge to discern genuinely beneficial services from those that are misleading. Additionally, regulatory oversight is crucial to ensure that the financial products and services being offered are transparent, fair, and truly in the best interest of the consumer, safeguarding against potential exploitation in an increasingly accessible financial market.

Privacy

Open banking provides citizens with digital autonomy: the agency to control who has access to their data and what it can be used for.[67] It introduces a paradigm where consumers are theoretically afforded more privacy-preserving options, as it decentralizes the financial services ecosystem and gives users more control over their data. A core privacy principle is that increased transparency into the information entities collect about individuals and what it is used for, insight available because of data portability, empowers those individuals to make more informed decisions around the data they share. By enabling consumers to dictate who can access their financial information and for what purpose, open banking

[66] Experian, "The Consumer Credit Information Report and Energy Utility Credit," White Paper (2019), https://perma.cc/G37E-3AW7.

[67] European Commission, supra note 55. Note that the majority of citizens respondents argued that financial service providers holding data should be obliged to share them with other financial or third-party service providers, if consumers have given their consent or agreement (55 percent; 30 out of 55 replies).

could enhance personal data autonomy. For instance, a consumer could choose to share their transaction data with a budgeting app while keeping it hidden from other types of services, tailoring privacy settings to their preferences and needs.

Additionally, open banking allows the introduction of new third parties whose competitive advantage is premised on the fact that they are more privacy oriented than traditional banks. For example, blockchain solutions can obscure user data in ways that might frustrate law enforcement efforts, but they offer robust privacy protections to users who do not wish to share their purchasing histories with companies or the government. Open banking can also facilitate the development of new, innovative, privacy-preserving technologies or solutions such as variable recurring payments[68]—technology that allows customers to authorize payment providers to draw on their bank funds on a recurring basis without having to share bank or payment information with each individual transacting business. This allows consumers to move away from predatory models like credit cards with high interest rates, while also minimizing the number of entities to whom they provide valuable and exploitable financial information.[69]

However, this new era of financial services also brings forth significant privacy risks. Regulatory mandates that were not designed with privacy in mind have vastly expanded the number of entities that can request customer financial information without a proactive system of ensuring these entities are responsible, secure, and privacy protecting. As consumer data becomes accessible to a multitude of new entities, including fintech startups, third-party payment services, and other nonbanking financial institutions, the surface area for potential data breaches and unauthorized data use expands. Many of these new entrants might not have the same level of robust data protection practices that traditional banks are mandated to have, due to either resource constraints or differing priorities. The risk is not merely theoretical; the more entities that have access to sensitive financial information, the higher the likelihood of a privacy breach.

Additionally, open banking could lead to new types of privacy exploitation and contribute to the disparate impact of these privacy harms on marginalized communities—and the current regime is unlikely to safeguard against it. The populations that turn to fintech solutions likely include marginalized communities currently excluded from the financial sector, which means their data is more vulnerable to exploitation. Without privacy measures built in to regulation, there is nothing stopping fintech companies from monetizing or misusing the data they have access to, just as the problematic

[68] Open Banking Implementation Entity, "Variable Recurring Payments: What Are They and How Can They Help SMEs?," https://perma.cc/WXD3-QV7G.

[69] Alexandre Gonthier, "From Lockdowns To Inflation: Consumers Are Primed For Open Banking," *Forbes* (Jan. 6, 2023).

financial gatekeepers have been doing for decades.[70] Data that was thought to be private might be manipulated to deny services or credit,[71] discriminatorily adjust prices, or push predatory products, micro-targeting advertising to disadvantaged communities[72] Similarly, new types of data could be created and sold—and who knows that that data might look like or might be used for.

Moreover, the complexity of consenting to data sharing in an open banking environment poses a substantial challenge for consumers. Privacy regulations largely assume privacy is protected by "notice and consent," or the requirement that companies share with consumers the data they collect and what it is used for. But most consumers do not read financial privacy notices or understand them.[73] Understanding and managing consents for multiple third-party providers to access various types of financial data will be even more challenging. Consumers will be faced with the intricate task of navigating what they are consenting to, which entities are receiving their data, and for what specific purposes these entities will use their information. This complexity could lead to consent fatigue, where consumers might inadvertently agree to data sharing practices that they do not fully understand or support, undermining the very privacy the system aims to protect.

Security

Open banking could significantly advance security. Legacy banking systems, often characterized by outdated technology and infrastructure, present significant security risks for several reasons. First, these systems were designed and built in an era before the current sophistication of cyber threats, meaning they lack the necessary defenses against modern hacking techniques and malware. Their outdated nature makes them inherently vulnerable to security breaches and financial fraud, as they may not support the latest encryption standards or have the capacity for regular, automated security updates that are critical in defending against contemporary cyber threats. Moreover, the complex patchwork of systems that has evolved in traditional banks—where newer systems are built on top of or integrated with older platforms—can create security loopholes and blind spots. These vulnerabilities are not merely technical

[70] Deloitte, "Open Banking: The Privacy and Security Imperative" (July 17, 2018), https://perma.cc/7K95-HUUH.

[71] Shashi Ran, Angus Duncan, Richard Peers, Aman Kohli, & David Phelps, "PSD2 and Open Banking: Using Regulation to Kick-start the Transformation of Banking," 18 (2017) ("The huge wealth of deep insight into customer behavior that can be gained through analysis of spending history, financial health and financial products owned could be a lucrative source of income for those controlling access to it.").

[72] See Saule T. Omarova, Professor of Law, Cornell University Law School, Testimony Before the Senate Committee on Banking, Housing, and Urban Affairs, "Fostering Economic Growth: Regulator Perspectives on Financial Technology (FinTech)," 115th Cong. (Sept. 18, 2018), https://perma.cc/XSM4-3W3S.

[73] See Justin Brookman, "Protecting Privacy in an Era of Weakening Regulation," 9 *Harvard Law & Policy Review* 355, 356 n.8 (2015); see also Alessandro Acquisti, Curtis Taylor, & Liad Wagman, "The Economics of Privacy," 54 *Journal of Economics Literature* 442, 479–80 (2016).

challenges; they represent significant risks to customer data privacy, financial assets, and the integrity of the financial system at large.

The lack of incentive for big finance institutions to update their systems and improve service quality can often be attributed to their dominant market control. When institutions hold a significant market share, the competitive pressure to innovate or invest in newer, more secure technologies is diminished. This complacency is bolstered by the high costs and operational disruptions associated with overhauling legacy systems. Such financial institutions may calculate that the immediate costs of modernization outweigh the perceived benefits, especially if their dominant position appears to secure their customer base and profitability in the short term. This situation creates a perverse incentive structure in which, despite the known risks and inefficiencies of legacy systems, the drive to invest in more secure, efficient, and customer-friendly technology is dampened. It underscores a systemic issue within the financial sector, where the slow pace of innovation and improvement in service quality can be linked directly to a lack of competitive pressures. This not only perpetuates the security vulnerabilities inherent in outdated systems but also hinders the overall advancement of the financial services industry toward more inclusive, innovative, and secure offerings.

Fintech companies, unencumbered by outdated legacy systems that often plague traditional banks, are in a prime position to adopt more advanced, secure technologies from the outset. This advantage allows them to leapfrog older, more vulnerable systems and implement cutting-edge security measures that can better protect against modern cyber threats. By prioritizing investment in secure alternatives, such as end-to-end encryption, secure cloud services, and robust authentication mechanisms, fintech firms can offer a level of data security that might surpass that of traditional banking institutions. This focus on security not only benefits consumers by safeguarding their financial information but also serves as a competitive edge for fintech companies in the financial services market.

Even if fintech companies are not security experts, open banking mandates will still improve security by facilitating direct interoperability between banks and fintech companies through secure APIs, as opposed to less secure methods like screen scraping, mentioned earlier. Screen scraping, in which third-party services access bank data by mimicking a user logging into their bank account, presents numerous security vulnerabilities, including the risk of exposing login credentials and financial data to interception.[74] Additionally, screen scraping frustrates the banks' ability to prevent fraud, when the bank is unable to distinguish among its client, the third party that has valid consent to access the data, and a malicious third party.[75] Open banking's API-based data sharing eliminates the need for these precarious

[74] See, e.g., *Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461 (N.D. Cal. 2021) (holding that the plaintiffs "adequately stated claims for intrusion and violation of the California Constitution's right to privacy" because of Plaid's allegedly lax security structures).

[75] Basel Committee on Banking Supervision, "Principles for the Sound Management of Operational Risk" (June 2011), https://perma.cc/5RWL-PTT6.

practices, enabling a secure, controlled exchange of information in which data is accessed and transmitted directly between institutions without exposing user credentials or unencrypted data.

Open banking, if extended to require interoperability of functions, such as user authentication in addition to data sharing, can allow for third parties to offer consumers the services they are best positioned to while reserving important and resource-intensive services, such as authentication and data storage, for the parties best positioned to do that. While consumers have already benefited substantially from the introduction of fintech startups, some of these startups can have less expertise and fewer resources related to privacy and security. Function availability through APIs can allow a fintech company to build a platform that analyzes spending habits without having to build a system to authenticate users, one of the most important aspects of good cybersecurity. It can also stream consumer data across institutions to present a user with their spending information without having to store that information permanently and therefore subject themselves to the increased risks of cyberattacks. As a result, consumers can lean on preexisting bank resources and expertise rather than having to trust unknown third parties, which may be trusted to provide a useful app but not to store credential information. This would increase the adoption of fintech solutions, by assuaging user privacy and security concerns related to these relatively new third parties.[76]

Open banking also promises to reduce fraud in the banking industry. In 2021, consumers in the United States lost more than $5.8 billion to fraud, which is a 70 percent increase from 2020.[77] Data access and transparency can allow for more insight into suspicious activities and the ability to trace the digital footprints of fraudulent transactions. Open banking facilitates the sharing of financial data between banks and authorized third-party providers via secure APIs. This shared access to financial data allows for more comprehensive monitoring of transactions across different services and accounts in real time. By analyzing patterns and behaviors across a wider data set, financial institutions and third parties can more accurately detect anomalies that may indicate fraudulent activity, enabling quicker intervention. The open banking ecosystem also encourages innovation in new fraud detection and prevention services. These services can leverage advanced technologies such as artificial intelligence and machine learning to predict and prevent fraudulent transactions with greater accuracy than traditional fraud detection systems.

Still, there remain broad security concerns about the openness of APIs in such a system. As it pertains to open banking, cyberattacks in Australia have raised concerns about whether banks are ready to cope with the new open banking requirements.[78] Introducing APIs, which function as doors into proprietary

[76] Id.

[77] Annie Nova, "Consumers Lost $5.8 Billion to Fraud Last Year, Up 70% Over 2020," CNBC (Feb. 22, 2022).

[78] Akamai Technologies, "Enemy at the Gates: Analyzing Attacks on Financial Services," Akamai Technologies (2019), https://perma.cc/2DK8-BZLQ.

systems, can introduce new threat vectors for bad actors to exploit. Moreover, there was a burst in attacks on APIs last year, according to research from cloud services and security company Akamai. Attacks on financial service APIs and web applications (which are closely related to APIs) more than tripled globally (257 percent growth), and in North America they more than quintupled (449 percent growth). [79] And there are further concerns about whether open banking could propel greater fraud and money laundering with easier peer-to-peer payments, consumer information, and invasive or obfuscating software.[80] The bottom line is that new, open technology creates new opportunities for cyberattacks and crime. That the technology involves hegemons of American finance and industry also creates a national security concern for banks and the financial system.

Transparency and Accountability

Open banking champions transparency, enhancing both public and governmental oversight into financial institutions. Easier access to financial data will lead to heightened scrutiny and accountability—and the ability for regulators and watchdogs to make better informed decisions. In an open banking ecosystem, diverse stakeholders, from users to the government, could access APIs directly, ensuring clarity and promoting trust. Where today the government and the public are limited by mandatory disclosures by banks, in an open banking regime, users, researchers, competitors, and the government can directly access APIs to understand what data is available and to whom. Additionally, further transparency to processes and shared information at universities, agencies, or industry groups can drive competition, resulting in better products and services for consumers. A focus on improving the industry could also facilitate a more inclusive financial system, potentially providing underserved populations with more access to banking services.

The transparency facilitated by open banking, while beneficial for consumer choice, competition, and regulatory oversight, can inadvertently become a tool for exploitation in the hands of authoritarian or surveillance-heavy regimes. These governments could leverage the detailed financial data accessible through open banking to enhance their surveillance capabilities and exert greater control over their citizens. In regimes where the government exercises tight control over financial institutions and technology companies, open banking can provide a centralized point of access to vast amounts of personal financial data. This data could be used to monitor citizens' activities, track political dissidents, or suppress dissent by analyzing transaction patterns, donations, and financial interactions that could indicate opposition to the regime.

Even in a country with more stringent privacy safeguards, there is still cause for concern. Open banking frameworks that facilitate cross-border data sharing can also raise concerns about the international

[79] Id.

[80] Tony Wicks, "8 Risks Open Banking Poses for Financial Crime Compliance," FICO (Jan. 23, 2020), https://perma.cc/MNG6-JXJP; Deloitte, "Open Banking in Europe: A Comprehensive Guide to Banking APIs" (2019), https://perma.cc/ED9J-UJ6V.

transfer of financial data to jurisdictions with poor human rights records. This could extend the reach of authoritarian regimes, enabling them to surveil and control citizens even beyond their borders.

Efficiency, Innovation, and Competition

Open banking and interoperability foster a financial ecosystem that significantly enhances efficiency, innovation, and competition. By enabling secure, standardized access to financial data across institutions through APIs, open banking reduces the friction associated with developing and delivering new financial services. This environment encourages fintech companies and traditional banks alike to innovate, creating more personalized, efficient, and diverse financial products. For consumers, this means access to a wider range of services that better meet their individual needs, often at lower costs due to the increased competition among providers. For countries, the bolstered innovation and competition translate into more dynamic financial sectors that can contribute to growth in gross domestic product (GDP). Some researchers have predicted that economies that embrace open banking can see GDP gains between 1 and 5 percent by 2030, with the economic benefits reaching not only financial institutions but also consumers.[81] A more efficient and competitive financial services market can increase consumer spending and saving options, optimize capital allocation, and enhance overall economic productivity by providing businesses with improved financial management tools and access to funding.

Interoperability and the unbundling of financial services contribute directly to lowering barriers to entry in the financial sector and reducing switching costs for consumers. Traditionally, consumers might have been reluctant to explore third-party financial solutions due to the inconvenience of moving away from their primary banking services. However, with open banking, consumers can seamlessly integrate services from multiple providers, retaining the usability and convenience of their main bank while benefiting from the specialized services offered by fintech companies. This ease of integration means that consumers no longer have to choose between the comprehensive service package offered by a traditional bank and the innovative solutions provided by fintech firms—they can have the best of both worlds. The reduced barriers to entry encourage more startups and tech companies to enter the financial services market, further driving innovation and consumer choice. Meanwhile, the lower switching costs empower consumers to pursue the best financial products for their needs, fostering a more consumer-centric financial marketplace that prioritizes value, quality, and convenience.

Moreover, financial institutions can harness open banking for enhanced efficiency and cost reductions, which can eventually benefit consumers. For instance, the integration of interoperable technology can reduce transaction costs through data sharing. As such, consumers might face fewer fees in areas such as

[81] Olivia White, Anu Madgavkar, Zac Townsend, James Manyika, Tunde Olanrewaju, Tawanda Sibanda, & Scott Kaufman, "Financial Data Unbound: The Value of Open Data for Individuals and Institutions," McKinsey & Company (2021), https://perma.cc/B439-M3PL.

currency conversion—a welcome development given the lack of transparency in the fee sector.[82] Similarly, India's open banking framework slashed transaction costs dramatically.[83]

However, as we argue in this paper, the benefits of open banking to competition are unlikely to be realized if implemented against the existing landscape of hegemonic power by a handful of large companies. The largest players in the financial sector, whom the initiative aims to balance power away from, might actually stand to gain the most from it. Despite bearing the brunt of compliance costs associated with implementing open banking protocols, these dominant banks and big tech companies possess the extensive resources and infrastructure necessary to capitalize on the new regime effectively. With more resources at their disposal, big banks currently have the upper hand in developing API open-banking-type technology with their resources, creating a "digital divide."[84] They are also well positioned to quickly observe, replicate, or even acquire innovative financial solutions developed by promising third parties. This ability to mimic or absorb innovation stifles competition and maintains big banks' market dominance, contrary to the goals of open banking.

Beyond the traditional banking sector, big tech Goliaths with existing large customer bases and data analytics capabilities also stand to gain more than startup fintech Davids.[85] They can use their technological prowess and customer insights to create financial products that are highly personalized and integrated with their other services, making them more attractive than those offered by smaller startups. Meta and Amazon already have services that could be easily integrated into an open banking system—and these big firms have the funds to make a mark. This gives big tech a significant advantage, potentially allowing them to dominate the burgeoning open banking ecosystem alongside the big banks.

This dynamic underscores a critical concern: While open banking is designed to democratize the financial services industry and spur innovation by lowering barriers to entry for smaller players, the actual beneficiaries may be the current market leaders—big banks and big tech companies. These

---

[82] European Commission, supra note 55. Consider, for example, that when European citizens were asked whether the cost of fees in general was clear, 35 percent (23 replies) disagreed, of which 24 percent (16 replies) strongly disagreed. For payments that involve a currency conversion, the feedback is even more negative: 46 percent (30 replies) found unclear what exchange will be applied, against only 14 percent (9 replies) who found it clear.

[83] N. Natarajan, "Use of Aadhaar for KYC Authentication Will Cut Costs," Hindu Business Line (April 11, 2016), https://perma.cc/GKJ9-B3ZP.

[84] Ben Pimentel, "The Group Pushing Fintechs to Play Nice With Banks," Protocol (Jan. 22, 2021), https://www.protocol.com/fintech/fdx-financial-data.

[85] Committee on Payments and Market Infrastructures and the Technical Committee of the International Organization of Securities Commissions, "Harmonisation of Critical OTC Derivatives Data Elements (Other Than UTI and UPI) – Third Batch," Bank for International Settlements (March 2019), https://perma.cc/64HB-PQG3.

entities can utilize their superior resources, data, and customer reach to overshadow the innovative contributions of smaller startups, the very entities that open banking seeks to empower. As a result, without careful regulation and measures to ensure fair competition, open banking may inadvertently reinforce the market power of the largest players, undermining its objectives to enhance competition, innovation, and consumer choice in the financial sector.

LOOKING FORWARD AT U.S. OPEN BANKING

The United States is in the begging phase of open banking adoption. But the demand for it is clear. Fintech is growing and innovating rapidly. The estimated number of consumers who have utilized a service affected in some way by consumer-authorized data sharing may be as large as 100 million, and the number of consumer and small business accounts accessed by authorized third parties is estimated to be 1.8 billion internationally.[86]

This industry growth has been met with attention from regulators. In July 2021, President Biden signed the Executive Order on Promoting Competition in the American Economy, actively encouraging the Consumer Financial Protection Bureau to craft rules under Section 1033 of the Dodd-Frank Act in support of open banking.[87] Subsequently, the CFPB announced in October 2023 that it was considering proposals that would require a defined subset of Dodd-Frank Act–covered persons that are data providers to make consumer financial information available to a consumer or an authorized third party.[88]

The proposed rule, known as the Personal Financial Data Rights Rule, aims to accelerate the shift towards open banking by:

- Requiring banks and other providers to make personal financial data available, at no charge to consumers or their agents, through dedicated digital interfaces that are safe, secure, and reliable.[89]

[86] See Financial Data and Technology Association (FDATA), "Competition Issues in Data Driven Consumer and Small Business Financial Services," 11 (June 2020), https://fdata.global/north-america/wpcontent/uploads/sites/3/2020/06/FDATA-US-Anticompetition-White-Paper-FINAL.pdf. Further, the EY Global FinTech Adoption Index shows that in 2019, 46 percent of digitally active U.S. consumers were "fintech adopters," up from 17 percent in 2015 and 33 percent in 2017. EY, Global FinTech Adoption Index, 6 (2019), https://www.ey.com/en_us/ey-global-fintech-adoption-index.

[87] Executive Order No. 14036, 86 Federal Register 36987 (July 9, 2021).

[88] Consumer Financial Protection Bureau, "CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking" (Oct. 27, 2023), https://perma.cc/PMY8-Q52S.

[89] Personal Finance Data Rights Rule § 1033.201(c)).

- Granting consumers a legal right to share their data, allowing them to grant third parties access to information associated with their credit card, checking, prepaid, and digital wallet accounts.[90]
- Enabling consumers to walk away from bad services and products, allowing them to more easily shift their data to a competitor offering better or lower priced products and services.[91]
- Instituting robust protections to prevent unchecked surveillance and misuse of data, requiring third parties to limit data collection, use, and retention to what is reasonably necessary to provide the consumer's requested product.[92]
- Providing meaningful consumer control by giving people the right to revoke access to their data, requiring data access to end immediately and deletion to be the default practice upon revocation.[93]
- Encouraging a move away from risky data collection practices like screen scraping.[94]
- Ensuring fair industry standard-setting by containing requirements to ensure industry standards are fair, open, and inclusive.[95]

It is this last section, 1033.141, that could hinder the implementation of these other promising proposals. Section 1033.141 empowers the CFPB to recognize standard-setting bodies of issuers of qualified industry standards. The bureau does not set forth an express set of provisions it would use to recognize these bodies but provides a vague set of criteria: whether it is open to all interested parties, whether decision-making is balanced across interested parties, whether it has written and publicly available policies and procedures, whether it has an appeals process, whether decisions are made by consensus, and whether its standard-setting process is transparent.

Absent from this consideration is whether the body takes into account the U.S. banking sector's highly concentrated nature, and the risk the industry, as it currently is comprised, could have on a burgeoning decentralized technology.

One of the key players in developing open banking APIs is the Financial Data Exchange (FDX), a nonprofit industry standards group that seeks to develop common, uniform, and interoperable standards

---

[90] *Id.* §§ 1033.201(a), 1033.211

[91] *Id.* §§ 1033.201(a), 1033.211

[92] *Id.* § 1033.421(a)-(c)).

[93] *Id.* § 1033.421(h))

[94] *Id.* § 1033.311(d)).

[95] *Id.* § 1033.141.

for financial data sharing in the United States and Canada.[96] FDX, founded in 2018, comprises over 200 members, including the biggest banks in the United States, fintech companies, and consumer groups.

Twenty-two million consumer accounts are currently using the FDX API for financial data sharing in the U.S. and Canada.[97] And a recent partnership between Wise US Inc. and Plaid Inc. exemplifies the benefits of interoperability between banks and financial services platforms.[98] These policies are welcome, but concern remains over whether the proposed FDX regime would create adequate safeguards to mandate pro-competitive adoption by big banks.

FDX's governance and makeup lean toward the existing players. Its leadership is made up mostly of representatives of the big banks—J.P. Morgan Chase and Bank of America. Its push for interoperability has not led to the promised proliferation of third-party providers, as promised. Rather than seeing numerous competitive offerings of financial products and services, we see a handful of power data aggregators serving as the intermediaries between traditional financial institutions.[99]

For instance, Plaid, an integrative financial technology, has amassed substantial power, providing API connectivity to more than 12,000 financial institutions and over 5,500 fintech firms.[100] Because interoperability with data aggregators like Plaid is optional today, the financial institutions that have agreed to work with Plaid have less incentive to work with other data aggregators. And, given that Plaid's value increases with each additional user, its network effects will entrench its position in the marketplace. This should set some alarm bells ringing as the U.S. expands its system, because haphazard calls for decentralized finance may lead to the rise of a handful of data aggregators like Plaid as opposed to the robust marketplace of evenhanded competitors originally envisioned by open banking advocates.[101]

Open banking presents both real promise to solve the gatekeeper problem in finance and real risks to consumer and public welfare.[102] Implemented poorly, though, the promise of open banking could

---

[96] Financial Data Exchange, "About FDX," https://perma.cc/NN8B-Q4K6.

[97] Financial Data Exchange, "22 Million Consumers Using FDX API" (Nov. 17, 2021), https://perma.cc/B5FD-74KB.

[98] Digital Transactions, "FDX Seeks to Make Open Banking More Accessible With Its Standard and API" (Feb. 24, 2022), https://perma.cc/ZNV3-KDJX.

[99] Awrey & Macey, supra note 60, at 43–49.

[100] Id.

[101] Id.

[102] Tyler Pathe, "Bank of American Leverages Open Banking to Introduce Account-to-Account Payment Solution," *FinTech Times* (Feb. 16, 2022), https://perma.cc/FEL6-S3T9.

backfire, leading to *reduced* privacy, security, and competition in the financial sector and beyond.[103] A decentralized platform does not automatically mean diffused risks and is not a panacea for all industry woes.[104] One just has to look at decentralized cryptocurrency finance and its front-running, coin and value manipulation,[105] security lapses,[106] liquidity issues,[107] and complete lack of privacy.[108]

In prior notices, the CFPB seemed aware of the competition problems in top-down implementation, saying that:

> To thrive, standard-setting organizations must not skew to the interests of the largest players in the market. They must reflect the full range of relevant interests—consumers and firms, incumbents and challengers, and large and small actors. In consumer finance, powerful firms have sometimes looked to manage emerging technologies through utilities, networks, or standard setting organizations skewed to their interests—or even owned by them.
>
> Control of the open banking system by such players threatens competition and the consumer's control of their own financial affairs. While the CFPB intends for the market to play a significant role in developing and maintaining open banking standards, it will pay close attention to any attempts to limit consumers' exercise of their data rights, particularly where such attempts proceed from coordinated efforts by dominant firms.[109]

---

[103] See Nicola Cetorelli & Philip E. Strahan, "Finance as a Barrier to Entry: Bank Competition and Industry Structure in Local U.S. Markets," 61 *Journal of Finance* 437, 437 (2006) ("The empirical evidence ... strongly supports the idea that in markets with concentrated banking, potential entrants face greater difficulty gaining access to credit than in markets in which banking is more competitive.").

[104] Schneider, supra note 7.

[105] See Class Action Complaint, Docket Number 1, *Ryan Huegerich et al. v. Kimberly Kardashian et al.,* No. 2:22-cv-00163, (C. D. Cal. Jan. 7, 2022) (class action unfair competition suit against various Instagram influencers for aiding in an alleged crypto pump-and-dump scheme).

[106] Mercedes Tunstall, "FBI Warns About Cybersecurity Problems on DeFi Platforms," Cadwalader, Wickersham & Taft LLP (Sept. 2, 2022), https://perma.cc/FQY8-ETDL.

[107] Sky Jung, "Privacy in Decentralized Finance: Should We Be Concerned?" *Harvard Technology Review* (Aug. 22, 2021).

[108] JP Konig, "The Privacy That DeFi Needs to Succeed," *CoinDesk* (Jan. 27, 2022), https://perma.cc/95NH-XH4Z.

[109] Rohit Chopra, "Laying the Foundation for Open Banking in the United States," Consumer Financial Production Bureau (June 12, 2023), https://perma.cc/Y2DL-TAD3.

These words are a good start, but implementation without proper consideration of competitive harms could lead to problems well beyond data rights—in privacy, security, and growth.

We suggest these requirements to accompany the CFPB's rollout to ensure that the U.S. can foster a more equitable and competitive financial ecosystem. In broad strokes, these would entail:

- Entrusting the development of open banking standards and APIs to a diverse group of stakeholders, including industry experts, scholars, and digital rights activists, to ensure the system serves the public interest rather than corporate interests.
- Implementing tiered regulatory compliance requirements that consider the size and resources of financial entities, offering smaller startups reduced compliance burdens or technical and financial support to meet open banking standards.
- Regulating the fees charged for access to banking APIs to ensure they are not prohibitively high for smaller entities, preventing large banks and tech companies from setting prices that only they can afford.
- Requiring reciprocity in data sharing among large financial institutions and big tech companies, ensuring that the benefits of open banking are mutual and not one sided.
- Establishing innovation hubs that provide funding or grants specifically aimed at supporting fintech startups, helping to level the playing field by giving startups the tools, guidance, and financial support they need to innovate and grow.
- Investing in consumer education programs that help users understand the benefits and risks associated with using fintech services, driving competition by encouraging the adoption of services offered by startups.

Additionally, merger attempts between banks and fintech firms should undergo rigorous antitrust scrutiny by the Department of Justice and the Federal Trade Commission (FTC). Big banks must be bound by stringent disclosure requirements to provide clarity on how they implement protocols and manage data, shedding light on any upstream benefits they may experience from third-party access to their information and whether these benefits are being exploited anticompetitively. Agencies like the FTC and the Securities and Exchange Commission should adapt their existing financial disclosure policies to the nuances of open banking to ensure transparency, bolster consumer trust, and prevent open banking from disproportionately benefiting incumbents over third parties or the public.

These principles are not limited to open banking. Interoperability in any industry will need to reckon with these factors and rectify the preexisting conditions that are antagonistic to interoperability. As the most robust set of interoperability measures today, open banking offers lessons to future interventions—in both its successes and its failures in achieving the conditions necessary for effective interoperability. Interoperable systems should not be met with centralized control.

CONCLUSION

The rise of centralized platforms and the concentration of power in the hands of a few dominant players pose significant challenges to competition, innovation, and consumer welfare across various industries. As these gatekeepers amass and exploit vast amounts of data, they create closed ecosystems that hinder the promise of interoperability, stifle the growth of smaller competitors, and limit consumer choice. Interoperability and data portability mandates represent potential solutions to decentralize power and foster a more open, competitive landscape.

However, the effectiveness of these regulatory interventions depends on a careful consideration of the specific context in which they are implemented. The open banking case study examined in this paper serves as an example of how the success of interoperability initiatives can be influenced by preexisting market conditions and the design of the regulatory framework.

In the financial sector, the high level of consolidation and the presence of dominant incumbents pose significant challenges to the implementation of open banking. Without addressing these underlying issues, interoperability mandates risk entrenching the power of large banks and tech giants, as they possess the resources and influence to shape standards and maintain their market dominance. Smaller, innovative players may struggle to compete on an uneven playing field, undermining the goals of increased competition and consumer choice.

To ensure the success of interoperability initiatives, policymakers must adopt a holistic approach that combines technological solutions with measures to decentralize decision-making power and create a level playing field for all market participants. This may involve fostering diverse stakeholder participation in standard-setting processes, implementing tiered compliance requirements, regulating access fees, and promoting reciprocity in data sharing.

Furthermore, interoperability frameworks must strike a delicate balance between enabling data sharing and protecting consumer privacy, security, and autonomy. Robust safeguards and meaningful consumer control over data are essential to prevent misuse and maintain trust in the system.

The lessons learned from open banking extend to other sectors grappling with the challenges of centralization and the potential of interoperability. In health care, for example, the concentration of patient data within a few dominant electronic health record providers could hinder the exchange of information across health care providers, limiting the potential for improved care coordination and patient outcomes. Similarly, in the social media landscape, the dominance of a few platforms leads to the creation of walled gardens that restrict user choice and limit the growth of alternative networks.

Across these diverse contexts, the success of interoperability initiatives will depend on carefully designed frameworks that account for market realities, prioritize consumer welfare, and foster a competitive and innovative ecosystem.

Ultimately, although interoperability and data portability mandates hold immense promise for decentralizing power and promoting competition, their implementation is not a panacea. The open

banking case study highlights the complexities and potential pitfalls that must be navigated to ensure the success of these initiatives. By learning from these experiences and adopting a holistic, context-specific approach, policymakers and industry stakeholders can craft effective interoperability strategies that unlock the full potential of data sharing, foster innovation, and drive positive change across various sectors. As we move forward in an increasingly data-driven world, striking the right balance between openness and protection will be crucial to building a more equitable, competitive, and consumer-centric digital landscape.

The Digital Social Contract paper series is supported by funding from the John S. and James L. Knight Foundation and Meta, which played no role in the selection of the specific topics or authors and which played no editorial role in the individual papers.