THE EMERGENCE OF FINANCIAL DATA GOVERNANCE AND THE CHALLENGE OF FINANCIAL DATA SOVEREIGNTY

Giuliano G. Castellano, Ēriks K. Selga,** and Douglas W. Arner****

Abstract: This chapter addresses the challenges of datafication of finance and financial data sovereignty. Section II considers the datafication of finance. Section III considers the intersection of data, finance, and data governance, highlighting emerging general data governance styles. Section IV highlights the intersection of financial data regulation and personal data regulation in the context of the evolution of a range of Open Banking strategies focusing on personal financial data. Section V presents four emerging financial data governance strategies, exemplified by the United States, EU, China, and India, seeking to bring together finance and its regulation with their evolving domestic data governance regimes. Section VI elaborates on how the result of differences in these strategies combined with prudential objectives converges toward territorialization via data localization. Section VII addresses this growing challenge of fragmentation by outlining how the well-developed transnational regulatory frameworks in finance offer an opportunity to develop technological solutions and approaches that may, in fact, support both the objectives of financial and data regulation.

Keywords: financial data governance, data sovereignty, data regulation, personal data, financial regulation.

This is an updated pre-print version; the final version of this book chapter (Open Access):

Castellano, Giuliano G., Ēriks K. Selga, and Douglas W. Arner, 'The Emergence of Financial Data Governance and the Challenge of Financial Data Sovereignty', in Anupam Chander, and Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford University Press, 2023), pages 178-210.

Available here: https://doi.org/10.1093/oso/9780197582794.003.0009

* Associate Professor of Law and Deputy Director, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

** Research Fellow, Asian Institute of International Financial Law, Faculty of Law, University of Hong Kong.

*** Kerry Holdings Professor in Law, RGC Senior Fellow in Digital Finance and Sustainable Development, Senior Fellow – Asia Global Institute, and Associate Director – HKU-Standard Chartered Foundation FinTech Academy, University of Hong Kong, Senior Fellow, Melbourne Law School, University of Melbourne, Australia.

I. Introduction

The essence of the Fourth Industrial Revolution is digital transformation. The "digitalization of everything" combines two interrelated processes. First, a process of digitization transforms analog information into digital form.[1] Second, datafication is converting every aspect of modern life into digital data that is gathered and analyzed through a range of rapidly evolving technologies and methods, including increasingly artificial intelligence (AI).[2] Digital transformation continues as communications, computing, processing, and data storage technologies become ever more available and powerful, connecting billions of people and their interactions across the world.[3] The COVID19 crisis accelerated the process, triggering unprecedented creation, collection, aggregation, and dissemination of—and most crucially—dependence on data.[4]

Data is thus a strategic priority. Like other strategic assets—land, energy, food, water, capital[5]—governments are seeking to assert sovereign control in an emerging era of multipolar geopolitical competition. Through the implementation of new data-specific policies and regulation, general data governance frameworks are emerging, defining a new set of rights and obligations for stakeholders such as data generators and owners. As analyzed elsewhere, the general data governance styles of the largest economies—the EU, the United States, and the People's Republic of China—collide, threatening the paradigm of free transnational data flows and fragmenting the global economy.[6]

Finance is also highly dependent on data and its transnational movement. Since the invention of the telegraph in the 19th century, finance has grown into perhaps the most globalized and digitized but also regulated sector of the modern economy.[7] Underlying this digital transformation, the financial sector has undergone a process of dematerialization of financial assets and processes over the past 50 years, transforming financial products and information into digital data.[8] Hence, financial entities,

---

[1] On digitization, *see* VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA 78 (2013).

[2] On datafication, *see* Ulises A. Mejias & Nick Couldry, *Datafication*, 8 INTERNET POL'Y REV. (2019).

[3] See Ross P. Buckley et al., *Regulating Artificial Intelligence in Finance: Putting the Human in the Loop*, 43 SYDNEY L.J. (2021)

[4] Especially in in the context of digital communications, interactions, payments, commerce, and finance, see DOUGLAS W. ARNER ET AL., DIGITAL FINANCE, COVID-19 AND EXISTENTIAL SUSTAINABILITY CRISES: SETTING THE AGENDA FOR THE 2020S, NO. 1 (2021).

[5] As indicated by *The Economist* in 2017: "[t]he world's most valuable resource is no longer oil, but data." *Data Is Giving Rise to a New Economy*, ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy

[6] Douglas W. Arner et al., *The Transnational Data Governance Problem*, 37 BERKELEY TECHNOL. L.J. 623 (2022) (discussing the various regulatory and policy clashes taking place that are inhibiting free transnational data movement).

[7] Douglas W. Arner et al., *The Evolution of Fintech: A New Post-Crisis Paradigm*, 47 GEO. J. INT'L L. 1271 (2015) (presenting a framework for the globalization of financial transactions enabled by financial technology).

[8] Dematerialization is a central phenomenon in finance, propelling financial globalization as noted by Campbell Jones, *The World of Finance*, 44 DIACRITICS 30 (2016); and financial innovation, as indicated

consumers, and regulators routinely share data (in digital form) to provide their services and maintain the stability and integrity of the financial system. This dependence of finance on data flows in an environment of growing autonomous data regulation rules raises complex questions regarding how data governance and financial regulation interact and what the implication is for a digitally globalized financial system.

This chapter thus seeks to address the challenges of datafication of finance and financial data sovereignty. Section II considers the datafication of finance. Section III considers the intersection of data, finance, and data governance, highlighting both emerging general data governance styles. Section IV highlights the intersection of financial data regulation and personal data regulation in the context of the evolution of a range of Open Banking strategies focusing on personal financial data. Section V presents four emerging financial data governance strategies, exemplified by the United States, EU, China, and India, seeking to bring together finance and its regulation with their evolving domestic data governance regimes. Section VI elaborates on how the result of differences in these strategies combined with prudential objectives are converging toward territorialization via data localization. We then address this growing challenge of fragmentation in Section VII by outlining how the well-developed transnational regulatory frameworks in finance offer an opportunity to develop technological solutions and approaches that may, in fact, support both the objectives of financial and data regulation.

II. The Datafication of Finance

Finance is inextricably linked to the acquisition, analysis, and processing of massive volumes of diverse forms of information, which today are mostly digital. Capital markets can be conceptualized as networks of social relationships where participants send signals about the quality and quantity of different financial products, thus determining their prices. More broadly, financial information, intended as data concerning transactions of businesses and individuals, is the core fuel of modern financial systems. Financial information underlies both the Efficient Capital Markets hypothesis as well as financial regulatory requirements for information disclosure, access, and quality. In addition to investors in stock markets who rely on analysis of information to make investment and trading decisions, lenders, for instance, estimate the creditworthiness of potential borrowers through a variety of financial information, such as repayment history, credit card transactions, income statements, and asset information. A wide range of proprietary but also shared sources such as credit rating agencies, credit bureaus, and increasingly a range of Big Data and alternative data sources compound such sources of data, exemplified in the rise of FinTech and BigTech credit.

Finance, technology, and law are co-developmental, paralleling and interacting with the evolution of past and modern civilization.[9] Since the invention of paper in China

by Patrice Baubeau, *Dematerialization and the Cashless Society: A Look Backward, a Look Sideward, in* THE BOOK OF PAYMENTS 85 (Bernardo Batiz-Lazo & Leonidas Efthymiou eds., 2016).

[9] Finance can be traced back to ancient Sumer, whereby grain and ingots of copper and silver were used as payment. Financial transactions were codified in the Babylonian Code of Hammurabi circa 1800 B.C.

(2,000 years ago) until the late 1970s, finance was an industry based on paper: paper ledgers, paper certificates, and paper money (in addition to coins).[10] With electrification, the diffusion of electronic storage, and computing power, finance evolved into a digital industry, where financial instruments (such as stocks and other securities) are dematerialized, and financial information is digital.

In this context, the law evolves and interacts with finance technology. As financial assets, such as securities, are dematerialized and, thus, exist and are held electronically in depository systems, legal rules have had to adapt. The legal status, the evidentiary nature, and the enforceability of electronic transactions must correspond to the needs of market participants and function at least as well as those attributed to paper-based transactions. While most of the legal issues concerned with the emergence of electronic financial activities have been debated and, to a large extent, addressed, since the second half of the 20th century, 11 new challenges have emerged as the processes of dematerialization ushered a more profound and ongoing transformation. These have been clearest over the past decade with the emergence of new technologies in finance, in particular, new forms of digital assets.

To unlock the potential of digital finance, regulatory policies have been focusing increasingly on facilitating the circulation of data within and across financial industries. In addition to traditional focuses on standardization and regulatory sharing, a notable new example is offered by Open Banking initiatives, whereby payment and banking service providers should ensure that authorized third parties can have access to customer and payment account information. While complying with this core objective, however, financial institutions and jurisdictions can adopt a variety of approaches, selecting the level of openness, the type of services, and how to integrate their offerings with the business model of other players. The result is a financial system where financial data becomes a resource to expand the reach of financial services and a commodity that should be integrated into new financial services.

Financial data is a broad but distinct form of data. It includes traditional banking data, transaction history, and other information typically tied to individual accounts and users. Such data is used for various purposes, including for the assessment of various risks—based on models calculating the probability of repayment—and for the pricing of different services. It also refers to data about financial markets and products, such as stock prices and accounting data about firms and governments. In a similar vein, the data gathered by financial institutions is routinely used for regulatory purposes: financial institutions are required to gather data to detect suspicious activities in the fight against money laundering, and financing of terrorism and market, client, statistical, and transaction data are used determine the level of protection against various prudential risks, including credit risk, market risk, and operational risk.[11]

For more, *see* George Levy, *A Brief History of Finance*, *in* COMPUTATIONAL FINANCE USING C AND C# 275 (2016).

[10] *Id.*

[11] For discussions exemplifying regulatory reporting requirements for financial data, *see* Abdullahi Usman Bello & Jackie Harvey, *From a Risk-Based to an Uncertainty-Based Approach to Anti-Money Laundering Compliance*, 30 SECUR. J. 24 (2017); PATRIK ALAMAKI & DANIEL BROBY, THE EFFECTIVENESS OF REGULATORY REPORTING BY BANKING INSTITUTIONS (2019).

Financial data thus pertains to a variety of classes of data. It includes non-personal data used by financial services and their clients to send instructions for payments transnationally, to report to regulators, or to interact with clients. It also comprises personal data with information tied to any individual account, transaction, or other sensitive information.

The breadth and depth of financial data, as well as the critical character of the financial sector itself to jurisdictions, makes its regulation a priority. The challenge is that regulating financial data requires coordinating several policy aims concurrently. For instance, financial data must be sufficiently pliable to support its use by the financial services industry while affording sufficient protection to the growing amounts of personal and public data.

III. Financial Data Governance and General Data Governance

Financial data governance encompasses a variety of rules and principles that can be grouped into three categories.[12] The first category of components comprises regulatory regimes designed to govern the production, acquisition, use, and circulation of financial data. These rules are core aspects of traditional regulatory policies aimed at ensuring market efficiency, consumer and investor protection, financial stability, and market integrity. Such rules cover most aspects of finance and have had to continually evolve as a result of technological evolution and digitalization, including industry, regulatory, and customer data. The second category comprises broader data governance styles. These styles are autonomous sets of rules and principles designed at the domestic level to extend sovereign control over data, data flows, and infrastructure. These emerged initially in the context of personal data but are now being extended more broadly for a range of reasons, including national security, competitiveness, and developmental objectives. The third category encompasses a range of emerging regulatory initiatives, strategies, and models for digital finance, such as Open Banking policies focusing on personal financial data, which have been developed to address challenges and opportunities of the digital transformation of financial sectors. The coming together of a diverse range of traditional and novel regulatory regimes that are (directly or indirectly) concerned with financial data and the datafication of finance are evolving into a new governance framework for digital finance.

A. Regulating Financial Data

The regulatory framework for financial data is a manifestation of both the increased centrality of data in modern society and the digitization and datafication of finance. Hence, regulation affects financial data through two intertwined dynamics.

The first dynamic that defines the regulatory perimeter for financial data stems from the digitization of finance. Financial regulation has adapted to ensure that the risks

[12] Douglas W. Arner et al., *Financial Data Governance*, 74 HASTINGS L.J. 235 (2023) (introducing the notion of "financial data governance")

related to the growing reliance on digital information, financial assets, and related infrastructures are properly addressed. The gathering, processing, management, and use of financial information in digital form has, thus, become central to financial regulatory policies concerned with the solvency of financial institutions, the stability and the integrity of the financial system at large. Hence, regulatory regimes concerned with the digitization of finance have evolved around prudential regulation, conduct of business rules (with particular attention to AML requirements), and supervisory initiatives.

In respect to prudential policies, strong attention has been given to the risks emerging from the growing integration of digital systems in financial activities. Technological failures, cyber-attacks, legal actions, and regulatory sanctions related to the mistreatment of data are forms of operational risk that may compromise the solvency of financial institutions. As data and technology are inextricably related to finance, new international standards have been elaborated to ensure that technology-related operational risks are properly addressed. In particular, the Basel Committee on Banking Supervision (BCBS) has launched an epochal overhaul of the rules that banks must implement vis-à-vis the assessment and management of data and technology risk: TechRisk. The result is an increased level of capital requirements to ensure enough loss-absorbing capacity against operational risk and the implementation of a principle-based approach to strengthen operational resilience within banks.[13]

Lastly, financial data is becoming the direct corollary of broader regulatory reporting requirements and supervisory action. Regulators are requiring banking data to be machine-readable to enable supervisory automation processes and more granular data aggregation capabilities.[14] Many regulatory initiatives enacted after the 2008 Global Financial Crisis require financial institutions to report a large set of data on individual operations, such as security-by-security and loan-by-loan reporting.[15] Regulatory and supervisory technology (RegTech / SupTech) models are requiring financial data to be structured so that regulators have direct access via automatically packaged business data (data-input approach), through collecting business data directly from bank systems (data-pull approach), through analyzing operational bank data at will (real-time access), or other formats. These RegTech / SupTech instruments are not only expanding the micro-prudential supervisory capacity but enabling the aggregation of vast data pools for machine learning and AI solutions used for risk management.

[13] Capital requirements for operational risks are enshrined in the Consolidated Basel Framework; with the new rules the ability of banks to use own estimations to assess capital requirements is limited; see CONSOLIDATED BASEL FRAMEWORK (Basel Committee on Banking Supervision ed., Comprehensive version ed. 2019). In addition, with the last revision of the Principles for Operational Resilience, the BCBS issued an updated guidance on operational risk to include information and communication technology risks, including cybersecurity, but also to require the sound structuring of data, especially in regard to third-party service providers; see REVISIONS TO THE PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK (Basel Committee on Banking Supervision ed., Comprehensive version ed. 2021) at 7.

[14] FINANCIAL STABILITY BOARD, THE USE OF SUPERVISORY AND REGULATORY TECHNOLOGY BY AUTHORITIES AND REGULATED INSTITUTIONS (2020).

[15] TORONTO CENTER, FINTECH, REGTECH AND SUPTECH: WHAT THEY MEAN FOR FINANCIAL SUPERVISION (2017).

Second, as data is treated as a strategic resource and governance expands its reach domestically and internationally,[16] regulatory regimes concerned with the treatment of financial information naturally intersect and interact with general data policies. In fact, financial data encompasses myriad classes and types of data that, while used for financial purposes, may also fall squarely into the general category (or categories) of data, particularly personal data. The holders and processors of financial data are thus being increasingly directly or indirectly regulated by general data governance rules in force in any given jurisdiction. These general regimes typically establish different rights concerned with the alienability, circulation, or management of personal financial data. However, at the same time, financial data—both personal and non-personal—are also the object of specific regulatory initiatives, stemming from sector-specific needs and concerns.

B. The Evolution of Data Governance Styles

In the past 30 years, economic globalization has been supported by a common approach to data. Originating from a U.S.-led conception, the digital world developed as a permissionless, open, and liberal space, as evidenced by the Internet. Here, individuals, corporate entities, state actors, and international organizations converged in a global network of networks.[17] Upon these premises, market-like mechanisms gathered and exchanged data that, in turn, became the primary commodity in the digital space. As the links between digital and physical worlds multiplied, owing to the development of new technologies and to the expansion of infrastructural capabilities, a data economy developed and expanded beyond the digital perimeter. From daily tasks and personal and professional capacities of individuals to critical societal functions, such as payment and healthcare systems, societal dependence on data has become ubiquitous.

As data becomes a strategic asset, nation-states have begun to assert sovereignty over the digital world, both domestically and internationally. Legal and regulatory frameworks are being developed to define rights and obligations for data generators and holders.[18] Competition policies have been triggered to curb data abuse by dominant incumbent firms.[19] New rules to assert control over internal and external data flows and

[16] Especially, and increasingly in regard to critical infrastructure, and critical functions like national security, financial markets, or transportation. *See* Arner et al., *supra* note 6.

[17] The Internet has been described a burgeoning "Network of Networks" that enables interaction between many different domains. *See* Sara Helen Wilford et al., *The Digital Network of Networks: Regulatory Risk and Policy Challenges of Vaccine Passports*, 12 EUROPEAN J. OF RISK REGULATION 393 (2021); WILLIAM H. DUTTON, MULTISTAKEHOLDER INTERNET GOVERNANCE? (2015).

[18] Rights and obligations for data stakeholders extends across many policy domains. *See generally* Rene Abraham, Johannes Schneider, & Jan vom Brocke, *Data Governance: A Conceptual Framework, Structured Review, and Research Agenda*, 49 INTERNATIONAL J. OF INFO. MGMT. 424–38 (2019).

[19] For instance, the FTC recently filed a complaint against Facebook in an ongoing federal antitrust case, alleging that Facebook resorted to illegal buy-or-develop schemes to maintain market dominance. See Federal Trade Commission, *FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush (last visited Aug. 22, 2024)

related infrastructure are being enacted.[20] At the heart of these initiatives lies the urge for state actors to assert their sovereignty over data.[21] The result is the emergence of an increasingly fragmented global data governance framework.

Taken together, the domestic efforts to reign in the digital world define specific patterns. As argued elsewhere, such patterns create specific data governance styles.[22]

Crucially, data governance styles manifest in the cardinal direction taken to regulate data, data flows, and digital infrastructures within and outside domestic borders. When applied to the three major world economies and primary standard-setters—notably, China, the EU, and the United States—the domestic trajectories for data governance emerge starkly. Starting from the United States, it is clear that a market-based style and a laissez-faire regulatory approach to data and technology have nurtured the rise of the Internet and its current paradigm: globalized, permissionless, and supportive of free trade.[23]

Largely in response to the dominance of American players in the global digital economy, the EU, first, and China, more recently, have developed their own digital strategies. In the EU, the governance style is right-based as it establishes protections for the gathering, use, and circulation of personal data of EU citizens while spurring the emergence of a digital economy within the European Single Market.[24] A more centralized governance style is emerging in China, where a state-based approach treats data and data flow as part of broader policies, ranging from national security and infrastructural autonomy to general socioeconomic goals of improving the quality of life of Chinese citizens.[25] The analysis of data governance styles can be extended to other jurisdictions. For example, India is a jurisdiction where data governance focuses on a rights-based approach while also embracing utilizing data policy as the main vehicle for the delivery of public goods and services.

Each data governance style connects and interacts with the strategies to regulate financial data and digital finance in various manners. In particular, as financial data encompasses a variety of different classes of general data, from personal to non-personal information, the emergence of data governance styles necessarily intersects with rules and principles designed to regulate financial data and its related ecosystem. More

[20] These interventions cover a variety of areas of law and are related to asserting control for the purposes of privacy, competition, socioeconomic development, and other reasons. For more, *see* Arner et al., *infra* note 36.

[21] OECD, THE PATH TO BECOMING A DATA-DRIVEN PUBLIC SECTOR (2019) ; UN SECRETARY-GENERAL, DATA STRATEGY OF THE SECRETARY-GENERAL FOR ACTION BY EVERYONE, EVERYWHERE WITH INSIGHT, IMPACT AND INTEGRITY, 2020–22 (2020)

[22] The locution has been first coined in Arner et al., *supra* note 6.

[23] *Id.*

[24] Brett Aho & Roberta Duffield, *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*, 49 ECON. & SOC'Y 187 (2020)

[25] FAZHI ZHENGFU JIANSHE SHISHI GANGYAO (2021–2025) (**法治政府建**设实施纲要 (2021–2025 **年**)) [Implementation Outline for the Construction of a Government Under the Rule of Law (2021–2025)] (promuglated by Central Comm. CCP & St. Council, Aug. 11, 2021), http://xinhuanet.com/2021-08/11/c_1127752490.htm (China).

broadly, as data is the object of financial transactions, data governance styles represent a major influence as the financial data governance strategies are developed. Depending on whether a given data governance style promotes or inhibits the digitization and datafication of finance, financial data governance will result in complementarities or exceptionalisms. This connection is particularly evident in the context of Open Banking initiatives, as they presuppose the circulation of data within a given jurisdiction.

IV. Open Banking

Financial data is thus impacted directly by both financial regulation and also by general data governance styles. In an increasing range of aspects, frictions, overlaps, and conflicts are emerging in the relationships between the two regulatory regimes both within and across different jurisdictions.

For instance, unlike the EU, which has had a formal legal framework for personal data since 1995,[26] the United States has not had a general legislative framework governing personal data but rather a complex series of federal and state legislation and case law. California adopted the first comprehensive state data protection legislation in 2018, the California Consumer Privacy Act (CCPA), which entered into force in 2020.[27] However, the United States has developed legislation in a number of specific areas, including finance. The most significant are the Fair Credit Reporting Act enacted in 1970[28] and amended by the Fair and Accurate Credit Transactions Act of 2003[29] and the Gramm-Leach-Bliley Act[30] and its creation of the Consumer Financial Protection Bureau (CFPB)[31] specifically addressing consumer financial data. Absent a general data protection framework, these can be seen as sector-specific elements of the U.S. general data governance style—albeit ones that provide for a specific set of rules that may, in fact, eventually form the basis of a broader set of rules governing personal data in the United States.

In contrast, while the EU has long had a general framework for personal data protection, prior to 2018, this had a limited impact in the context of financial data, personal or otherwise. This, however, changed with the implementation of both PSD2

[26] European Data Protection Supervisor, *The History of the General Data Protection Regulation*, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Feb. 9, 2024) (describing the development of data protection in the EU).

[27] Ch. 55, 2018 Cal. Stat. 1807 (codified as amended at CAL. CIV. CODE §§ 1798.100-.199.100 (2020).

[28] Pub. L. No. 91-508, tit. VI, 84 Stat. 1114, 1127-36 (1970) (codified as amended at 15 U.S.C.Hi 1681-1681x (2018)).

[29] Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. § 1681 (2006))

[30] Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in sections of 12 U.S.C. and 15 U.S.C.).

[31] Jolina C. Cuaresma, *Commissioning the Consumer Financial Protection Bureau*, 31 LOY. CONSUMER L. REV. 426 (2018–2019) (discussing the unique leadership and accountability structure of the Consumer Financial Protection Bureau).

and GDPR in 2018.[32] PSD2 (adopted in 2015) provides a framework for Open Banking while GDPR (adopted in 2016) provides a comprehensive framework for personal data protection. Together they are central to both the EU's general data governance style and also its financial data governance strategy.

Open Banking parallels and interacts with the general data governance style but also is emerging as a separate yet related strategy, with the EU as first mover and the leading proponent of a mandatory legislative approach, reflecting and extending its more general data governance style. In the EU, PSD2 (which predates GDPR) establishes a framework that promotes the emergence of novel payment-service providers, through a licensing structure that requires banks to provide access to a client's payment account to third parties on the basis of their consent.[33] Banks have to comply with a system of rules that facilitate the transferability of data, by developing APIs that meet a minimum set of functional standards.[34] PSD2 however only mandates sharing by banks, an aspect for which is has been criticized.[35]

The Open Banking movement has now spread globally, albeit in a range of differing forms. To unlock the potential of the digital economy, jurisdictions are pursuing a range of Open Banking variants.

At the most basic level, Open Banking enables consumer generated data to be transferred (data portability) or accessed by third parties. Approaches can range from legislatively mandated (as in the EU) to industry-led voluntary systems (as in the United States), with a range of roles for regulators in between.[36] In mandatory systems like the EU, Australia and the United Kingdom, core granular provisions have been adopted, mandating financial institutions to grant third-party access to their data, regulating access through APIs, and establishing standardization of digital ID for users. The comparison with different rules offers a useful illustration of how policymakers in different jurisdictions understand and promote Open Banking: Open Banking in one jurisdiction can be very different from Open Banking in another, particularly in the context of its level of legal basis and its interaction with general data governance styles.

Data portability lies at the heart of Open Banking strategies; key variances lie in the degree of portability required. For instance, while U.S. federal law does not require information portability (and thus is the basis of a voluntary Open Banking strategy in the United States and one which so far has largely been ineffectual as a result of industry recalcitrance despite outward enthusiasm), the California Consumer Protection Act grants users a right to receive their personal information in a useable readable format for

[32] Douglas W. Arner et al, *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II*, 25 STAN. J.L. BUS. & FIN. 245 (2020).

[33] MICHAEL R. KING & RICHARD W. NESBITT, THE TECHNOLOGICAL REVOLUTION IN FINANCIAL SERVICES: HOW BANKS, FINTECHS, AND CUSTOMERS WIN TOGETHER 143 (2020).

[34] See EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in 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), OJ 2016 L119/1.

[35] Douglas W. Arner et al., *Open Banking, Open Data and Open Finance: Lessons from the European Union*, in Linda Jeng (ed), OPEN BANKING (2022)

[36] *See generally Id.*

easy transmission from their data holder.[37] The EU GDPR provides a similar right, highlighting that the copy of a user's data should be in a commonly used and machine-readable format. Both regimes establish a requirement for data holders to initially classify and compartmentalize personal data and to be able to divide it from the rest of their data.

The approach adopted to Open Banking in any given jurisdiction is an important proxy to gauge the trajectory being adopted for financial data governance. In general terms, Open Banking policies are typically concerned with regulating the relationships with (i) financial data holders, such as banks and other financial institutions; (ii) processors, such as technology-focused and FinTech firms; and (iii) users mostly represented by individuals and small business.[38]

These actors can be further divided into a set of subcategories. Data processors can be divided into those that can aggregate user-generated data but cannot use (or that cannot have access to such data), and payment service initiators that can perform transactions on behalf of customers. These relationships can take a variety of archetypal forms. Aggregators are typically banks and other financial institutions that combine services from third-party providers to enhance their offerings or provide new services. Financial institutions can also be "distributors," acting as service providers for a third-party processor that manages client interfaces. Other entities can offer data orchestration services, for instance, by bringing together data from multiple sources into a marketplace. The result is a data ecosystem that can be harnessed to promote more advanced and inclusive financial services.

Along with the EU, the United Kingdom and Australia[39] are typically seen as the strongest examples of legislatively mandated Open Banking strategies. In contrast, the United States is usually seen as a (so far largely ineffectual) example of an industry-led voluntary Open Banking strategy. The EU, in fact, is moving beyond Open Banking toward Open Finance and eventually Open Data, reflecting the parallel evolution of its general data governance style, as is Australia. In between these extremes lies a range of models, usually characterized by the level of regulatory guidance and involvement, with Singapore and Hong Kong both being characterized by active regulatory encouragement and standard-setting but absent legislative mandates. Singapore, in particular, has been very active in building infrastructure and implementing regulatory encouragement as the basis of its Open Banking strategy, suggesting the regulator-led approach as a third major form.

China is also developing its own variant of Open Banking. In China, much of the consumer-authorized financial data access occurs through private platforms. However, there are no laws expressly requiring consumer consent-based data sharing or financial portability. The Chinese government issued recommended rules on standard API specifications for commercial banks in 2020. These standards require banks to establish

[37] Ch. 55, 2018 Cal. Stat. 1807 (codified as amended at CAL. CIV. CODE §§ 1798.100-.199.100 (2020)).

[38] These are the core stakeholders in the open banking cycle, and consist of entities that generate, process, and hold data; see Yan Carrière-Swallow et al., *India's Approach to Open Banking: Some Implications for Financial Inclusion*, No. WP/21/52 (2021)

[39] Ross P. Buckley et al., *Australia's Data-Sharing Regime: Six Lessons for the World*, 33 KING'S LAW JOURNAL 61 (2022).

internal, enterprise, and external APIs, instead of just focusing on bank-to-customer interactions. The 2018 guidelines for data governance set out detailed architectural structures for the data management of financial institutions.[40] A more recent set of interim provisions stipulates minimum consent and requires that consent is requested if giving access to third parties.[41] It is emerging as a mandatory system, albeit with data as a common resource rather than one controlled by individuals or financial institutions.

Likewise, India is developing yet another Open Banking strategy, one based on individual control of data (as in the EU, United Kingdom, and Australia) but with its use facilitated via a system of aggregation via licensed data aggregators:[42] In India, Open Banking follows a data aggregator model. Firms licensed by the Reserve Bank of India act as fiduciaries, collecting customer's financial data and sharing it with their consent to third parties.[43] Following the objectives of financial inclusion and facilitating financial competition in the market, account aggregators are a public good that ensures a level playing field, precluding the accrual and appropriation of data management costs by individual institutions while allowing reciprocal data sharing. Through aggregate banking, the goal is to extend the India Stack from payments into credit, personal finance, wealth management, and insurance.

Thus, Open Banking is emerging in a variety of jurisdictional strategies, each designed to maximize the benefits of personal financial data, bridging financial regulation and general data governance styles and often modifying both.

V. Financial Data Governance Strategies

General data governance styles interact with financial regulation in the financial data governance model of any given jurisdiction. The main footprint left by each data governance style onto the financial data governance model pertains to the attribution of different degrees of control over data to one category of the societal actors populating the data ecosystem. The control over data, in general, and financial data, more specifically, is attributed by prioritizing (i) market dynamics, where data holders, such as business organizations and financial institutions, are key players; (ii) the interests of individuals, intended primarily as the data generators; or (iii) the public interests, representing the collectivity organized by state actors and public entities.

Through this prism, we identify three archetypical data governance models, based on which group of social actors is prioritized. These archetypes extend to financial data governance. In particular, the different levels of control attributed to societal actors

[40] China Banking and Insurance Regulatory Commission issued the "Guidelines for Data Governance of Banking Financial Institutions," available at http://gdjr.gd.gov.cn/gdjr/jrzx/jryw/content/post_2870321.html

[41] Interim Provisions on the Protection and Management of Personal Information of Mobile Internet Applications, available at http://www.cac.gov.cn/2021-04/26/c_1621018189707703.htm

[42] Shri Rao, Remarks by Shri M. Rajeshwar Rao, Deputy Governor, Speech at Reserve Bank of India (Apr. 14, 2021) (2021)

[43] Nandan Nilekani, *Data to the People: India's Inclusive Internet*, 97 FOREIGN AFF. 19 (2018).

over data influences the regulation of financial data and intersects with Open Banking policies. These three models are analyzed next.

A. Property-Based: United States

Central to a financial data governance model that is market-orientated is the notion that data is an asset that can be produced, priced, and exchanged. Essentially, data is addressed as property that is freely alienable. Regulatory interventions are limited and intended to promote confidence in the market while protecting the integrity and stability of the financial system. Access to and transfer of data are contractual matters, left to the free negotiation between parties. Property rights over data concerning accounts, payments, and transactions are retained by the financial institutions. Data generators, however, may be granted a right to data portability and can request third-party access.

This approach is epitomized by the general style adopted in the United States, where the market-based approach has favored the emergence of a diverse FinTech ecosystem. FinTech firms have and continue to obtain data without the involvement of other banks via credential-based access or "screen-scraping." Screen scraping is the use of software to read the user data inputs and outputs in their bank without drawing on the data from the bank's servers—it is a process that can be completed without the participation of a customer's bank. Though there is consensus that direct access to data via APIs is superior to screen scraping in the way of security, reliability, and user control—there is no binding regulatory input on how to address the issues of informed consumer consent, the scope, and duration of access, as well as the allocation of liability in case of data loss or misuse.

The industry takes the lead in establishing standards for open banking products and services. The Clearing House—a banking association responsible for core payments system infrastructure in the United States[44]—has proposed a Model Agreement standard created for data sharing between financial service providers. The aim is to transition from screen scraping to APIs. A more technical set of standards has been established by the Financial Data Exchange—a cross-section of banks, data aggregators, and technology companies created in 2018. These standards create an interoperable API for user-permissioned financial data sharing with over 600 financial data elements currently available, including banking, tax, insurance, and investment data.[45]

While the United States may be seen as the clearest example of the ideal of a market-based model for financial data governance, in reality, financial regulation in the United States—as highlighted above—has long addressed consumer protection in the

[44] The Clearing House is owned by the largest banks of the United States and has a daily clearing and settlement volume of two trillion U.S. dollars. *See* The Clearing House, *Our History*, https://www.theclearinghouse.org/about/history (last visited Jan. 9, 2024)

[45] Financial Data Exchange, *Home*, FINANCIAL DATA EXCHANGE, https://financialdataexchange.org/FDX/Home/FDX/Default.aspx?hkey=bd839735-ebf5-426a-91f9-8334cbae1438 (last visited Jan. 9, 2024); Oana Ifrim, *The State of Open Banking and Open Finance in the US and Canada – Interview with FDX (Part 1)*, THE PAYPERS, https://thepaypers.com/interviews/the-state-of-open-banking-and-open-finance-in-the-us-and-canada-interview-with-fdx-part-1--1253761 (last visited Jan. 9, 2024).

context of financial data. Therefore, the United States can be seen as the leading example of a market-based model for general data governance; however, in the context of financial data governance, it has developed a range of personal and other financial data rules designed to support market efficiency, consumer protection, and financial stability.

B. Rights-Based: European Union

An individual rights-based model for financial data governance prioritizes the control of individuals over market dynamics. Data is treated more as a right of individuals rather than as freely alienable property. The gathering, use, and transfer of data are regulated through statutory rights that canvas contractual negotiation and limit the transferability of data ownership and control over data. Separation of personal and non-personal data is generally key, as more restrictions are applied to the former category encompassing information that are deemed sensitive. Non-personal data is generally treated as alienable property.

This model is epitomized by the approach adopted in the EU. The general data governance framework of the Union has evolved around three core priorities: (i) a focus on individual rights and privacy, (ii) the prevention of data concentration in the hands of a handful of dominant firms, and (iii) the more recent promotion of sufficient technological capacity to favor the growth of the internal market. Starting with a series of data protection and privacy directives primarily focused on protecting consumers (EU citizens), the data governance framework expanded in scope and influence.[46] Most recently, both GDPR and PSD2 adopted a series of measures granting ownership and control of data to individuals.[47] The trajectory is poised to be maintained and reinforced with the EU-wide digital ID regime via the eIDAS regulation, which establishes a framework for digital access to cross-border public and private services in the internal market.

In this context, different regulatory regimes apply to non-personal and personal data. Non-personal data is generally alienable and can circulate freely.[48] Domestic authorities must be able to retain access to certain data even if located in different Member States, and data holders must implement measures to facilitate data portability procedures between service providers.[49] A different regime applies to personal data, which are inalienable from the individual they pertain to and regardless of any

[46] Thomas Streinz, *The Evolution of European Data Law*, No. ID 3762971 (2021) (presenting an overview of the burgeoning EU data governance framework).

[47] See Article 36 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/1 1O/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing 2007/64/EC, 2015 O.J. (L 337) 35, known as PSD2.

[48] Article 4 of Regulation 2018/1807 prohibits "data localization requirements" thus requiring free flow of data in the EU. See Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the EU [2018] OJ L303/59.

[49] Article 5 of Regulation 2018/1807 presents competent authorities with the right to "request, or obtain, access to data for the performance of their official duties . . ." and such requests can in practice require real-time access, and data localization. Article 6 encourages the development of "principles of transparency and interoperability" to facilitate switching service providers and the porting of data.

contractual agreement.[50] GDPR allows personal data to be exported, subject to the official recognition from the European Commission that the regulatory framework of the receiving (non-EU) jurisdiction ensures basic protections that are deemed equal to those applied in the EU.[51] Furthermore, Member States can enact data localization measures in the context of health, financial services, or other sectors.[52]

The allocation of control over data to individuals is a pillar of this system. In open banking strategies, individuals maintain control over their data, as financial institutions can share them with authorized third parties only if requested by customers.[53] Yet, financial institutions must ensure that the transfer of data can occur in a systematized fashion and in compliance with a set of minimum requirements.[54]

Built on this framework, the 2020 EU Digital Finance Strategy aims to create a digital Single Market to boost the scalability and competition between financial service providers.[55] This strategy includes enabling EU-wide interoperable use of digital identities to allow easier onboarding, suitability assessments, and the "re-use" of onboarding for other purposes beyond financial services. This data space will be centered on a new EU digital finance platform that enables industry and supervisory authorities to interact online, offering e-licensing procedures on the basis of the expanded onboarding regimes and data exchange.[56] One of the key strategies of the 2020 EU DFS is moving from "Open Banking" of PSD2 and GDPR to "Open Finance," in which all financial data must be freely transferable to third parties and eventually under the new EU Digital Strategy, moving to "Open Data," in which data are fully under individual control with the necessary standards and infrastructure to enable use.

---

[50] *See* EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons in 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), OJ 2016 L119/1.

[51] *Id.*

[52] *Id. See* NIGEL CORY ET AL., PRINCIPLES AND POLICIES FOR "DATA FREE FLOW WITH TRUST" (2019) (highlighting the limits of data protection under the GDPR); Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* (2017) (highlighting the transaction costs of data protection regimes).

[53] Article 64 of PSD2 expressly requires authorization of payment transactions to be considered only if the "payer has given consent to execute the payment transaction." *See supra* note 48.

[54] Articles 65–72 set out a variety of rules on the procedural aspects of, for example, initiating a payment on behalf of a client via a third-party service provider. *See id.*

[55] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European Strategy for Data*, COM (2020) 66 final (Feb. 19, 2020), https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf; REINER SCHULZE & DIRK STAUDENMAYER, EU DIGITAL LAW: ARTICLE-BY-ARTICLE COMMENTARY (2020); Despoina Anagnostopoulou, *The EU Digital Single Market and the Platform Economy*, *in* ECONOMIC GROWTH IN THE EUROPEAN UNION 43 (Christos Nikas ed., 2020); LUÍS CABRAL ET AL., THE EU DIGITAL MARKETS ACT: A REPORT FROM A PANEL OF ECONOMIC EXPERTS (2021), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122910/jrc122910_external_study_report_-_the_eu_digital_markets_acts.pdf .

[56] CABRAL ET AL., *supra* note 56.

C. Shared Resource: China

In jurisdictions adopting a shared-resource model, data is considered a shared resource that is managed and controlled by public entities in a centralized fashion. While market dynamics are still present and encouraged, private accumulation of power over data is limited primarily through direct public interventions. Protections are established for data generators (individuals) through the establishment of minimum rights. Yet, the ultimate control over data and related flows and infrastructures is left to public authorities.

China is the most emblematic case of a jurisdiction that is implementing a public-focused model. Characterized by a state-centric structure, the emergence of an internal market for data occurs when the interest of the collectivity is in view. Following the overarching developmental goal, enshrined in the notion of Common Prosperity,[57] data governance policy pursues a twofold objective. First, the recent emergence of a data governance framework is intended to pursue stability for social, economic, and financial purposes, while maintaining national security. Second, data policies aim at bolstering and supporting the competitive dynamics to promote innovation, through the development of an internal digital market.[58]

This twofold objective results in public-private relationships that evolved in a co-dependent manner. Prior to 2020, data was largely treated in a way that was functionally similar to the U.S. approach, whereby a small number of large firms gathered and traded data on consumer behavior, and the central control to curb excessive accumulation of power in private hands became more dominant with a series of legislative and policy interventions.[59] Furthermore, over the past decade, the domestic market was largely protected from foreign competition. This combination of factors led to the development of national champions, such as Alibaba, Weibo, Baidu, and QQ, as well as technical mechanisms to block data inflows and outflows. In fact, the existence of identified incumbent firms led to the developing institutional capacity for the central government to monitor a vast amount of data.[60] As a result, data flows, and access have been more easily governed and deployed as a part of a general strategy to achieve overarching policy goals, such as socio-economic stability, innovation, and growth.

[57] The "Common Prosperity" agenda was set in various official announcements. In particular, see CCCPC (Central Committee of the Communist Party of China) and SCC (State Council of China), 2021, "14th Five-Year Plan (2021–2025) for National Economic and Social Development and the Long-Range Objectives through the Year 2035."

[58] Rogier Creemers, *China's Conception of Cyber Sovereignty*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY 107 (D. Broeders & Bibi van den Berg eds., 2020).

[59] Together, the 2017 Cybersecurity law, 2021 Data Security Law, and 2021 Personal Information Protection Law limit private company dominance of data.

[60] China blocks access to 10 of the top 25 top global websites creating a parallel Internet for domestically dominant platform to flourish, *see* Sebastian Hermes et al., *Breeding Grounds of Digital Platforms: Exploring the Sources of American Platform Domination, China's Platform Self-Sufficiency, and Europe's Platform Gap*, ECIS (2020) (discussing the access dynamic between online platforms around the world).

Ultimately, the data circulating in mainland China amount to almost a third of global movements.[61]

In the past years, a "cyber sovereignty" framework has been developed and gradually enacted to promote innovation under a state-centric framework. The central pillars of this framework are three fundamental laws: the 2017 Cybersecurity law, 2021 Data Security Law, and 2021 Personal Information Protection Law (PIPL). The overall approach is reflected in a new State Council policy framework enacted in August 2021.[62] While control over data under the emerging system follows an individual-based model, similar to the one deployed in the EU—whereby personal data are inalienable and non-personal data can be freely disposed—ultimate control over data belongs to the central government. Not only does the government have access to data, it also mandates data collection and analysis in both the public and private sector, with a focus on enhancing the Social Credit Score as a central mechanism for monitoring. Moreover, although the government allows uninhibited flows internally, data can only leave or enter China with express government permission.[63]

This state-based data governance style extends to a shared banking paradigm and in fact has been implemented most directly in this context, with a series of regulatory interventions triggered by concerns about Ant Financial leading to a related series of regulatory changes specifically targeting Ant in some cases, addressing the financial sector more generally in others, and in some addressing data and cybersecurity requirements more generally. Financial data is treated as a public resource, under the control of the central government. The largest Chinese digital platforms and BigTechs are entrusted to gather data that feed into the users' social credit score and other credit, commercial and financial scoring systems, both public and proprietary. For this purpose data generated from dispute resolution cases, contract fulfillment, and other financial activities contribute to determine these various credit scores.[64] WeChat—an omnichannel platform with 1 billion active users owned by Tencent—feeds the information back to the Chinese government to build personalized emotional, behavioral, and physiological data and add to user health portfolios.[65] Similarly, the

[61] Aho and Duffield, *supra* note 25; Wei Yin, *A Comparison of the US and EU Regulatory Responses to China's state Capitalism: Implication, Issue and Direction*, 19 ASIA EUR. J. 1–25 (2021) (discussing the size of China's state-centric form of capitalism).

[62] Implementation Outline for the Construction of a Government under the Rule of Law (2021–2025), issued by the Central Committee of the Communist Party of China and the State Council, Aug. 11, 2021. Available at http://www.xinhuanet.com/2021-08/11/c_1127752490.htm.

[63] Angela Huyue Zhang, *Agility Over Stability: China's Great Reversal in Regulating the Platform Economy*, University of Hong Kong Faculty of Law Research Paper No. 2021/36 (2021) (highlighting China's expanding regulatory oversight via antitrust, financial, and data regulation).

[64] Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 102 MINN. L. REV. 1563 (2017).

[65] Michael Paulsen & Jesper Tække, *Acting with and against Big Data in School and Society: The Big Democratic Questions of Big Data*, 5 J. COMM. & MEDIA STUD. 15 (2020); Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUD. COMP. INT'L DEV. 45 (2021); Quan Li et al., *A Framework for Big Data Governance to Advance RHINs: A Case Study of China*, 7 IEEE ACCESS 50330 (2019); Lulu Yilun Chen, *China Considers Creating State-Backed Company to Oversee Tech Data*, BLOOMBERG (Mar. 24, 2021), https://www.bloomberg.com/news/articles/2021-03-24/china-is-said-to-mull-state-backed-company-to-oversee-tech-data .

Chinese authorities have provided express lists of essential and nonessential data that financial service providers can request from users.[66] More profoundly, with a recent regulatory intervention, the People's Bank of China, together with other financial supervisory authorities, ordered 13 of the largest technology firms to unbundle and restructure their business in order to separate the Internet-based activities from financial activities; to the undertake the latter type of activities a license is required.[67] As a result, financial services developed to support the data economy are brought squarely within the financial regulation perimeter to "break [the] information monopoly" and "enhance the sense of social responsibility."[68]

Thus, China is taking a very different avenue to the United States or EU, although all three are seeking to address similar concerns around financial stability, consumer protection, national security, competitiveness, and innovation.

D. Hybrid Models

Jurisdictions can be categorized depending on whether they prioritize market dynamics, individual rights, or public interests, resulting in archetypical models. In existing jurisdictional contexts, although different domestic approaches epitomize such archetypes, a balance between the interests of different categories of actors always occurs. This is to say that "pure" market-based, individual-based, and public-focused models for financial data governance do not exist. Each real-world model is, to a different extent, the result of a balance, where stronger priority is given more prominently to one of the three main constituencies. When the resulting model does not have a distinct prioritization, hybrid archetypes emerge. In particular, financial regulatory objectives interplay with general data governance objectives, resulting in novel combinations of financial data governance approaches.

As an example, India is emerging as a key leader in strategically harnessing the potential of the digitization and datafication of finance.

The Indian data governance approach reflects a hybrid model that prioritizes the allocation of control to individuals and the state. At the heart of this model is the need to increase financial and public services inclusion through digitalization, combined with a rights-based systems for data and combined with a general market framework.[69]

Over the past 10 years, India has introduced the multilayered digital infrastructure known as the "India Stack." India Stack is a strategy designed to put in place infrastructure to enable wider development, innovation, and digitalization across

---

[66] *China to Rein in Mobile Apps' Collection of Personal Data, Technology*, BUS. TIMES (Mar. 22, 2021), https://www.businesstimes.com.sg/technology/china-to-rein-in-mobile-apps-collection-of-personal-data.

[67] THE PEOPLE'S BANK OF CHINA, FINANCIAL REGULATORS HAVE JOINT REGULATORY TALK WITH INTERNET PLATFORM ENTERPRISES ENGAGED IN FINANCIAL BUSINESSES (2021) (the 13 firms include Tencent, Du Xiaoman Financial, JD Finance, ByteDance, Meituan Finance, DiDi Finance, Lufax, Airstar Digital Technology, 360 DigiTech, Sina Finance, Suning Finance, Gome Finance and Ctrip Finance.).

[68] *Id.*

[69] NANDAN NILEKANI, IMAGINING INDIA: THE IDEA OF A RENEWED NATION 140–52 (1st American ed. 2009) (arguing for IT infrastructure as one of the main enablers of the Indian economic growth)

India. It consists of a range of APIs, open standards, and infrastructure standards that enable access to a broad range of services digitally for Indian citizens.[70] Since 2011, over 90 percent of the Indian population has received a digital identity, and more than half of the identity holders have linked bank accounts to it.[71]

India Stack consists of four layers of infrastructure and standards. The digital identity layer, known as Aadhaar, links individuals to a unique identity number tied to their biometric identifiers—a photograph, fingerprints, iris scans, and demographic information. The second layer consists of the Unified Payments Interface (UPI), an API-based interoperable payments interface that can be used by banks and vendors to send money between financial service providers.[72] The third layer is the digitization of documentation and verification, allowing public and private sector participants to authenticate users and perform electronic Know-Your-Client procedures.[73] The last layer is the consent layer, which enables the active management of an individual's data through regulated intermediaries. The government has established, for instance, a voluntary standard consent-providing template that enterprises must use to replace opaque and unclear terms and conditions.[74]

The general financial inclusion ethos dovetails with the objective of promoting competition within the domestic financial sector.[75] The Indian financial landscape is dominated by state-owned banks, holding almost two-thirds of total banking assets.[76] By increasing ease of access to financial services—especially in cashless format—competition within its banking sector is expected to increase.[77]

The resulting hybrid model reflects a strong concentration of control over data infrastructure for broader economic, financial, and developmental purposes. Yet, the powers of state actors are curtailed within the Indian constitutional framework and India's approach to personal data embodied in a bill expected to be enacted in the near future.[78] In this regard, the Supreme Court decided that Aadhaar identities can be required to receive welfare benefits,[79] while also finding that mandatory linking of

[70] Carrière-Swallow et al., *supra* note 39 (describing the development of the India Stack and noting the upcoming "consent layer" as a further enabler of financial data governance).

[71] *Id.*

[72] NILEKANI, *supra* note 70.

[73] Carrière-Swallow et al., *supra* note 39.

[74] NILEKANI, *supra* note 70.

[75] RESERVE BANK OF INDIA, NATIONAL STRATEGY FOR FINANCIAL INCLUSION (2019).

[76] *Id.*

[77] Carrière-Swallow et al., *supra* note 39.

[78] Alpha law, *Update on Data Protection Law*, https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law (last visited Feb. 12, 2024).

[79] Utkash Anand, *4-1 Verdict: Supreme Court Dismisses Pleas Seeking Aadhaar Ruling Review*, HINDUSTAN TIMES, https://www.hindustantimes.com/india-news/41-verdict-supreme-court-dismisses-pleas-seeking-aadhaar-ruling-review-101611189869910.html (last visited Jan. 10, 2024).

Aadhaar accounts is generally unconstitutional with limited exceptions.[80] Banks, for example, are not allowed to deny service if the customer has no linked Aadhaar number.[81]

This general trend is reflected also in India's Open Banking strategy, based on account aggregators, whereby financial institutions are mandated to collect data and shared them with a third party. In this context, financial institutions act as fiduciaries to source data,[82] but they may not access, store, or further sell the acquired data.[83] Account Aggregators authenticate subjects using their Aadhaar ID and map the ID to the available documents in the third layer of the India Stack, gaining access and retrieving the subject's financial assets, liabilities, or cash flows.[84] Through these systems, they enable broader financial service origination, underwriting, disbursement, and payments.[85]

Through Account Aggregators, India is seeking to provide an interoperable data standard. The operational framework extends data sharing to more classes of data than other jurisdictions, lending availability to any data held in the India Stack. The broader aggregate banking approach is also not limited to the relationship between financial services providers and natural persons—the India Stack data is also used by and for legal persons, with no categorical distinction. However, there is no expectation to extend the notion of data aggregators to other areas like search and social media businesses.[86]

India's model can thus be seen as a hybrid approach to financial data governance and one that seeks to provide technological infrastructure to enable the aggregation and use of rights-based data while constraining the dominance of private sector platforms (whether banks or BigTech firms).

These emerging financial data governance models depict an increasingly localized international landscape, particularly for personal financial data. Reflecting the trend observed in the context of general data governance styles, fragmentation is steering the global data governance framework away from the traditional market-led approach that has underpinned the re-emergence of global finance in tandem with digitization since the 1970s. This trend is particularly evident in the context of financial data that are categorized as "personal" under domestic laws but are also increasingly impacting other forms of financial data.

---

[80] Ananya Bhattacharya Anand Nupur, *Aadhaar Is Voluntary—but Millions of Indians Are Already Trapped*, QUARTZ, https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/ (last visited Jan. 10, 2024).

[81] *Id.*

[82] Account aggregators are defined under Section 3 of the Reserve Bank of India Act. For a comment, see Directions regarding Registration and Operations of NBFC—Account Aggregators under section 45-IA of the Reserve Bank of India Act, 1934.

[83] *Id.*

[84] *Id.*

[85] Jame DiBiasio, *What Is the India Stack? Nandan Nilekani Explains*, DIGITAL FINANCE (Jul. 28, 2020), https://www.digfingroup.com/what-is-india-stack/.

[86] Carrière-Swallow et al., *supra* note 39.

VI. Financial Data Sovereignty: Localization vs. Globalization

The intersection between data, finance, law and regulation is not always harmonious. Financial data governance engenders potential conflicts between its core components. Finance is one of the most highly regulated industries, with complex networks of rules addressing financial stability, market integrity, market efficiency, and consumer protection.[87] A dense soft-law architecture ensures a minimum level of international coordination, with overarching policy objectives set by the Group of 20 and standards set by transnational regulatory bodies, such as the BCBS and the FSB. While the regulatory framework for financial data and the emergence of Open Banking initiatives tend to coexist cohesively with financial regulatory policies, the expansion of domestic data governance styles aimed at asserting jurisdictional sovereignty over data, their flows, and infrastructure creates new—at times incongruous—regulatory challenges.

A. Regulatory Fragmentation

In the context of financial data governance, coordination failures can take place at two different levels. At the first level, conflicts pertain to the policy objectives of financial and data regulation.[88] This is to say that at least one of the policy aims of data regulation, such as cybersecurity or privacy of individuals,[89] is at odds (or largely incompatible) with one or more of the policy objectives of financial regulation, such as financial stability, market fairness, and consumer protection or efficiency.[90] The second level of conflictual relationships comprises contrasts that, while not involving policy objectives, result in incongruencies between dispositive rules and principles,[91] such as those

[87] DOUGLAS W. ARNER, FINANCIAL STABILITY, ECONOMIC GROWTH, AND THE ROLE OF LAW (2007). Notwithstanding its potential benefits, integrating technology in finance creates new complexities that, in turn, may become a source of systemic risk. This is evident, for instance, in the context of digital banking services that allow depositors to withdraw their funds rapidly, generating a "digital bank run;" see Giuliano G. Castellano, *Don't Call It a Failure: Systemic Risk Governance for Complex Financial Systems*, LAW & SOCIAL INQUIRY (2024), 1, 25 doi:10.1017/lsi.2024.8 (noting the connection between law, technology, and financial systemic risk).

[88] Policy aims formulate the ordering criteria and shape the development of each law branch. These policy aims may be extrapolated from a range of diverse sources including statutes, regulatory principles, or case law. *See* Giuliano G. Castellano and Andrea Tosato, *Commercial Law Intersections*, HASTINGS L.J. (2021).

[89] In the United States, the right to privacy has been enshrined in the Privacy Act, which stringently regulates how the U.S. government collects data about individuals. See 5 U.S.C. § 552a; In the EU, the respect for private and family life and protection of personal data are a fundamental right enshrined in the European Charter of Fundamental Rights, see Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J.(C364) 1.

[90] This is considered a multi-core CLI coordination failure—one which is characterized by gaps or incongruences that stem from tension between the core spheres of two or more of the converging legal branches. *See* Castellano & Tosato, *supra* note 89.

[91] This is considered a "coordination failure" characterized by gaps or incongruencies stemming from tensions between different aspects of multiple branches of law. *See* Castellano & Tosato, *supra* note 89 at 1022.

establishing the non-alienability of personal data, or "operative prepositions,"[92] like the rules regulating APIs or the format and modes in which customers data must be collected.[93]

An example of a coordination failure of the first level involves the friction between privacy objectives, prudential rules, and the efficiency and transparency of payment systems. In cash payments, there is an innate element of full privacy owing to the inherent anonymity of cash-based transactions. However, such a degree of anonymity, which is a rich ground for money laundering activities, is not a feature of DLT payments.[94] In the context of central bank digital currencies (CBDCs), while anonymity (at least vis-à-vis regulators and enforcement authorities) is not an option, the protection of privacy is critical in many societal contexts.[95] As a public good, privacy is important to ensure a variety of outcomes, from preventing data-based price discrimination to ensure democratic functions.[96] For this reason, different forms of privacy measures have been considered, including regulatory techniques like government access based solely on the issuance of a warrant, or cryptographic methods that automate pseudo-anonymization. Nonetheless, each option requires a compromise, or a trade-off, between policy objectives.[97] A prioritization of privacy objectives will necessarily result in a subordination of financial regulation policies, aiming at ensuring the integrity, fairness, and efficiency of financial markets. In a similar vein, the sole pursuit of financial regulation policies would imply a way to lessen privacy protections. In the context of CBDCs, this is likely to result in a range of different structures reflecting differing balances of societal objectives.

However, it is AML that exemplifies the coordination challenge between data governance (data privacy and use) and financial regulation (financial integrity) dispositive rules most directly. AML rules seeks to minimize the criminal and terrorist use of the financial system and are thus based on identifying the identity of those seeking to access the financial system and the origin of their funds. It seeks to ensure that assets enter the economy licitly, under legal ownership. As such, AML regulation generally consists of numerous compliance rules for financial service provides but also establishes a growing list of predicate crimes and legal instruments to allow supervisors and law enforcement to detect, prevent, and otherwise combat money-laundering activity. Access to, and accumulation and analysis of financial and other forms of data is central

[92] Operative propositions are defined as the rules that "govern their subject matter with a high level of determinacy" and they are typically establishing key technical elements. *See* Castellano & Tosato, *supra* note 89 at 1045.

[93] For example, PSD2 requires the European Banking Authority to develop regulatory technical standards setting technical requirements to be used by payment service providers. *See supra* note 48 Art 98.

[94] Rodney J. Garratt & Maarten RC Van Oordt, *Privacy as a Public Good: A Case for Electronic Cash*, 129 J. OF POLITICAL ECONOMY 2157 (2021)

[95] Ellie Rennie & Stacey Steele, *Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency*, 3 LAW, TECHNOLOGY AND HUMANS 6 (2021).

[96] Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUROPEAN L.J. 140 (2019).

[97] Trade-offs require a prioritization of the policy aims of one branch over those of another. *See* Castellano & Tosato, *supra* note 89 at 1036.

to achieving the goals of both sides of the AML regime, yet this access is being restricted with increasing frequency by data privacy rules.

The international regulatory framework for AML focuses on the role of intermediaries (particularly financial intermediaries such as banks) and law enforcement agencies in collecting data to ensure compliance. AML measures by financial institutions are managed via a risk-based assessment (RBA) framework, as set by the main international AML standard-setting body—the Financial Action Task Force. Under the RBA, each financial services provider must create risk profiles for their clients, products, correspondent banks, and other parts of the financial service supply chain. These profiles feed off data that the bank must collect through its own sources, from B2B services, its own affiliates, public, or other sources. Law enforcement and financial intelligence agencies will likewise develop similar profiles.

An issue with dispositive rules and AML has emerged particularly in the context of Open Banking rules, most dramatically in the EU. Open Banking is a function of retail consumer ownership and/or control of their financial data. This ownership and/or control entails classifying an array of types of information, including creditworthiness, customer preferences, but also transaction histories. In the EU, PSD2—which mandates the Open Banking regime—provides a level of data protection for personal data, with an exception for processing personal data by obliged entities when "necessary to safeguard the prevention, investigation and detection of payment fraud."[98] However, a later law, GDPR, establishes a higher level of data protection that, while providing similar exceptions applies them particularly to processing personal data in "criminal cases," not collection.[99] In 2019, the European Data Protection Service (EDPS) requested the cease of operations of FIU.net—a core tool for the exchange of financial intelligence between Member States operated by Europol—due to a lack of status as criminals.[100] In early 2021, a similar conflict led the EDPS to require Europol to delete huge databases on individuals with no criminal status. Through these direct conflicts in approach, AML supervisors lost access to data to undertake their functions and share with regulated entities to construct in pursuit of their own obligations.

Thus, both from the standpoint of the industry seeking to comply with conflicting requirements of data regulation and financial regulation as well as from the standpoint of conflicting regulatory objectives resulting in suboptimal results, there is a need for a process of cross-consideration of objectives and contents in the context of data governance. It is no longer possible to use a siloed approach as it has evolved in the EU

[98] Art. 94.

[99] Art. 2 (2)(c).

[100] Foivi Mouzakiti, *Cooperation between Financial Intelligence Units in the European Union: Stuck in the Middle between the General Data Protection Regulation and the Police Data Protection Directive*, 11 NEW J. OF EUROPEAN CRIMINAL LAW 351 (2020) See also the recent discussion over a Judgment of the Court of Justice of the European in *WM and Sovim SA* to revoke public access to ultimate beneficial owner registries, highlighting the substantial risk the balancing adds to financial integrity. Mathias Siems, *Privacy vs shareholder transparency: did the ECJ decision in WM and Sovim SA impair the global fight against money laundering?*, 60 *Common Market Law Review* (2023) no. 4, 1137-1157

in the context of personal and financial data rules.[101] Financial data governance must seek to balance competing regulatory objectives.

This is also a pressing issue as both financial data governance and general data governance have extraterritorial reach to gain sovereignty over data and data flow beyond jurisdictional borders. The result is an increased compartmentalization of data.

B. Territorialization and Data Localization

The second set of challenges to the paradigm of global financial flows regards the growing tendency of data territorialization. Data territorialization is the demarcation of digital space. It involves asserting digital sovereignty via rules for data mobility, ownership, alienability, and other factors. Through the process of territorialization, jurisdictions seek to protect and maximize the value of domestic data in the context of their wider data governance strategy. These purposes can range from the establishment of national ID regimes for financial inclusion purposes, like India's Aadhar system, data localization requirements for certain types of data, as China requires for domestic and foreign companies in a range of sectors, or even the imposition of extraterritorial data rules, required for personal data under the GDPR. Financial data is also impacted by this process and its own objectives, particularly financial stability, national security, and competitiveness.

Unlike many other forms of data, financial data is—until recently—a partial exception to general trends of data territorialization. To allow access to international markets, and fulfill the derivative goal of financial stability, and the functioning of the economy itself, certain financial data are expressly free to traverse jurisdictions. This is best exemplified by the special status financial data receive in bilateral trade agreements, using those enacted by the United States, EU, and China as examples.

An example of the territorialization of financial data is Open Banking. Open Banking, by mandating certain technical levels of interoperability from banks, via data portability or API standards, integrates client financial data into a broader—usually domestic—data system.

More significantly, reflecting a trend away from the branch model and toward separately incorporated, capitalized, and regulated subsidiarity requirements in the aftermath of the 2008 Global Financial Crisis, similar trends toward "ring-fencing" and localization of regulatory, customer and risk management data of regulated financial institutions have emerged. In this context, an increasing range of financial regulators around the world are requiring not only customer data but also regulatory and risk management data locally or, at the least, ensure immediate and unconditional access of such data to regulators. With the digitalization of finance and the fact that an increasing range of financial businesses are not only digital but in fact digitally native, this is posing a significant challenge to the dominant operating paradigm of the global digital financial services industry: free flow of data enabling centralized control, use and analysis in pursuit of business objectives, risk management needs, and regulatory requirements.

[101] See Emilios Avgouleas & Alexandris Seratakis, *Governing the Digital Finance Value Chain in the EU: MIFID II, the Digital Package, and the Large Gaps between*, EUROPEAN CO. & FINANCIAL L. REV. (2021).

These data localization requirements are being driven by financial stability concerns (the need for regulators to access data in order to meet their mandates as well as to safeguard core systems of financial institutions and infrastructure, a major concern for over 20 years as a result of 9/11 and Y2K), by national security concerns (particularly relating to cybersecurity but also increasingly geopolitical), and by competitiveness concerns (maximizing the benefits of financial data in the context of an overall financial data governance strategy, increasingly in tandem with a wider general data governance approach).

The question emerging from financial data localization trends—resulting from a range of prudential, national security, and competitiveness concerns—is their significance. From the standpoint of the financial industry, such data localization requirements—particularly when the extraterritorial reach of one jurisdiction for data , for instance, in the context of a globally systemically important financial institution (G-SIFI) conflicts with localization requirements of another—are an impossible burden and one that will undermine both the benefits of cross-border finance as well as its regulation and risk management.

However, we argue that they are also problematic from the standpoint of the overall objectives of global financial stability, market integrity, and consumer protection.

VII. The Data Sovereignty Challenge

Will financial data territorialization, localization, and competition fundamentally challenge financial globalization? Or will data gaps and regulatory arbitrage due to financial data localization sow the seeds of the next financial crisis? We suggest that data localization will remain the status quo of financial data for various reasons. It is critical to the fulfillment of policy objectives, but it often lacks interoperability with the financial data of other regimes. The variety of licensing frameworks ensures that even the same entity may be generating different data in different jurisdictions.

Unlike transnational data governance,[102] global finance has a very well-developed framework for international cooperation and coordination. This framework provides a mechanism for cooperation in areas relating to transnational financial data. Existing mechanisms support standardization of disclosure and reporting requirements (essentially the framework for many forms of financial data creation and assurance) as well as cooperation in cross-border enforcement in both market conduct and market integrity, with well-developed cross-border cooperation and information sharing in the contexts of payments, banking, and securities.

As financial data harmonization increases, an expansion of current disclosure requirements due diligence rules is required. Necessarily, this will result in a more assertive utilization of RegTech and SupTech solutions that are capable of drawing on

[102] Arner et al., *supra* note 6; Institute of International Finance, *Strategic Framework for Digital Economic Cooperation* (2021) (arguing for the need of a new permanent structure to help guide international digital economic cooperation); VIKRAM HAKSAR CARRIERRE-SWALLOW, YAN, GIDDINGS, ANDREW, ISLAM, EMRAN, KAO, KATHLEEN, KOPP, EMANUEL, QUIROS ROMERO, & GABRIEL, TOWARD A GLOBAL APPROACH TO DATA IN THE DIGITAL AGE (2021) (presenting a case for global data policy frameworks).

more timely data, and combining data from a variety of sources to build prudential models about traditional and novel financial services.[103] These systems will increasingly depend on the coordination of several foundational infrastructures (like telecommunications), along with digital and financial infrastructures (like mobile data services, data repositories, and payment and settlement services) to facilitate the collection of data from new sources.

More profoundly, a stronger institutional framework at the international level might be needed. A key risk is that the fragmentation, in various guises,[104] will fracture the existing international financial architecture. The global financial architecture has continued to function more effectively than most other aspects of international cooperation and institutions owing to its continuous evolution. In general, as we have argued elsewhere, for areas beyond finance, a Digital Stability Board similar to the Financial Stability Board would provide an important cooperative mechanism going forward.[105]

Looking forward, important areas where shared interests are likely to support further financial data governance cooperation and harmonization include cybersecurity and other forms of TechRisk, and sustainability.

Perhaps the greatest opportunities, however, lie in new technologies.

In addition to the harmonization and a reinforced architectural framework supporting financial data governance, the financial sector is uniquely placed to develop technological solutions to the challenges of data localization and territorialization. Different technological systems have been developed.[106] All systems originate from the genesis format.[107] Under this model, the data collector has exclusive control over collected data.[108] However, there is an increasing range of variants being offered.

Jurisdictions could agree on pockets of rules for how and what data can be transferred and through which channels. A variety of technologies are already available to help secure such messages, from blockchain applications to security-by-design solutions that can help guarantee the security of transmission medium to AI that can

[103] GLOBAL FINANCIAL INNOVATION NETWORK, REGTECH & SUPTECH WORKSTREAM UPDATE (2021), https://static1.squarespace.com/static/5db7cdf53d173c0e010e8f68/t/601d7c09cbd7bc3255b685bf/1612545036876/GFIN_RegTech_SupTech_Workstream_Update+-+Final.pdf; Ioannis Anagnostopoulos, *Fintech and Regtech: Impact on Regulators and Banks*, 100 J. ECON. & BUS. 7 (2018).

[104] Mark Austen, *Addressing Fragmentation in Asian Markets: Data Localisation – GFMA's Data Privacy, Security and Mobility Principles* (2019); ASIFMA, *Addressing Market Fragmentation through the Policymaking Lifecycle* (2020) (presenting emerging examples of market fragmentation tied to sustainable finance, data privacy, AML compliance, and operational resilience).

[105] Arner et al., *supra* note 6; Institute of International Finance, *Strategic Framework for Digital Economic Cooperation* (2021) (arguing for the need of a new permanent structure to help guide international digital economic cooperation); VIKRAM HAKSAR CARRIERRE-SWALLOW, YAN, GIDDINGS, ANDREW, ISLAM, EMRAN, KAO, KATHLEEN, KOPP, EMANUEL, QUIROS ROMERO, & GABRIEL, TOWARD A GLOBAL APPROACH TO DATA IN THE DIGITAL AGE (2021) (presenting a case for global data policy frameworks).

[106] Bruno Carballa Smichowski, *Alternative Data Governance Models: Moving Beyond One-Size-Fits-All Solutions*, 54 INTERECONOMICS 222 (2019).

[107] *Id.*

[108] *Id.*

rapidly analyze the content of transmitted data. SWIFT, or other systems of payments messaging, or credit card messaging systems could adopt such a system. The data from local banks could transmit to a central standardized unit that automatically would process whether and where the data is allowed to route through in accordance with agreement by jurisdictions, similarly to how Qualified Trust Service Providers under the EU PSD2 regime certify digital ID certificates by pinging back to domestic authorities. These kinds of pockets will be vital for critical functions like cybersecurity, market integrity, and increasingly—sustainable financing, via technical, trust, and identification requirements for data transfers.

Concurrently, the private sector could facilitate the adoption of new technologies that would lessen regulatory tensions. These technologies use new techniques to reach the outcomes necessary for offering their products and services, without needing to interfere with or even directly access the data of other entities with or across jurisdictions. Federated data systems that divide bundles of data across many different systems can ensure that no party has a data monopoly,[109] whereby cloud data centers can ensure that it is always accessible though cloud infrastructure does raise separate financial stability, national security, and competitiveness issues of its own.[110] Through federated data analytics, banks and supervisors may not need to access the data of other parties at all, instead only requesting that they run the necessary portion of data analytics locally. Lastly, zero knowledge proof protocols enable secure responses from federated or decentralized data system without any access to or knowledge of the underlying data.[111] From the standpoint of infrastructure for financial data, blockchain and other decentralized structures therefore offer potential approaches, in particular from the standpoint of networking various data sources and enabling proprietary analytics but require a change in mindset about the nature and use of financial data.[112]

This change in mindset, technology, and policy approach would mean evolving from the dominant paradigm of financial data centralization to one focused on federated storage and analytics. We argue that, in fact, such a transition would not only be the best way to address the challenges of fragmentation of financial data governance but also to achieve the broader objectives of financial stability, market integrity, consumer protection, and market efficiency. More than any other, the financial services industry and its regulators are well-placed to make this transition, necessary as part of the ongoing datafication of finance and its regulation.

---

[109] World Economic Forum, *Federated Data Systems: Balancing Innovation and Trust in the Use of Sensitive Data* (2019) (discussing federated approaches to sensitive data in healthcare).

[110] See Financial Stability Board, *Third-Party Dependencies in Cloud Services Considerations on Financial Stability Implications* (2019); Financial Stability Board, *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion Paper* (2020) (presenting benefits and risks of third-party reliance).

[111] *See* Teresa Alameda, *Zero Knowledge Proof: How to Maintain Privacy in a Data-Based World*, NEWS BBVA (Sept. 11, 2019), https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/; Nihal R. Goawravaram, *Zero Knowledge Proofs and Applications to Financial Regulation* (2018) (introducing how zero-knowledge proofs can be used in finance via a variety of examples, mostly tied to disclosing information without showing financial holdings).

[112] Douglas W. Arner et al., *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, 20 EUROPEAN BUSINESS ORGANIZATION LAW REVIEW 55 (2019).