Articles

Financial Data Governance

DOUGLAS W. ARNER,[†] GIULIANO G. CASTELLANO,[†] ĒRIKS K. SELGA[†]

Finance is one of the most digitalized, globalized, and regulated sectors of the global economy. Traditionally technology intensive, the financial industry has been at the forefront of digital transformation, starting with the dematerialization of financial assets in the 1960s and culminating in the post–2008 global financial crisis era with the fintech movement. Now, finance is data: financial transactions are transfers of data; financial infrastructures, such as stock exchanges and payment systems, are data networks; financial institutions are data processors, gathering, analyzing, and trading the data generated by their customers. Financial regulation has adapted to this fast-paced evolution both by implementing new regimes and by adapting existing ones. Concomitantly, general data governance frameworks to protect a broad spectrum of interests, from individual privacy to national security, have emerged. Though these areas of law intersect, their relationship often remains unclear. This Article sheds new light in this critical area, focusing on key challenges and providing viable solutions to address them.

First, we define financial data governance as a heterogenous system of rules and principles concerned with financial data, digital finance, and related digital infrastructure. To explain how legal and regulatory regimes interact with the digitalization of finance, we consider the key emerging financial data governance styles in the European Union, People's Republic of China, India, and the United States. Second, we examine the challenges affecting financial data governance. While finance is inextricably linked to data governance, the coalescence of financial regulation, new regulatory frameworks for digital finance, and general data governance regimes is not always harmonious. Conflicts arising from the intersection of different uncoordinated regimes threaten to frustrate core policy objectives of stability, integrity,

---

[†] Kerry Holdings Professor in Law, RGC Senior Fellow in Digital Finance and Sustainable Development, Asia Global Institute Senior Fellow, and HKU-Standard Chartered FinTech Academy Associate Director, Faculty of Law, University of Hong Kong; Senior Visiting Fellow, University of Melbourne.

[†] 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.

Douglas W. Arner gratefully acknowledges the financial support of the Hong Kong Research Grants Council Senior Research Fellowship Scheme and the Qatar National Research Fund. Giuliano G. Castellano further thanks the Hong Kong Research Grants Council for generous support through the General Research Fund (GRF n. 17607119).

and security, as well as the functioning of the global financial system. Addressing this requires a reconceptualization of the financial data centralization paradigm, both by regulators and by the financial industry.

TABLE OF CONTENTS

INTRODUCTION

The essence of the ongoing Fourth Industrial Revolution is digital transformation. The "digitalization of everything" combines two interrelated processes, namely, digitization and datafication. Digitization transforms analog information into digital form.[1] Datafication is converting every aspect of modern life into digital data gathered and analyzed through a range of rapidly evolving technologies and methods.[2] These two processes are the propellers of digital transformation, whereby communications, computing, processing, and data-storage technologies become ever more available and powerful, connecting billions of people across the world.[3] The COVID crisis has accelerated the process, triggering unprecedented creation, collection, aggregation, dissemination of, and—most crucially—dependence on data.[4] As economic and social processes become increasingly underpinned by data transfers, data itself is becoming the foundation of numerous critical societal functions, including healthcare, transportation, commerce, national security, and finance.[5]

Data is thus a strategic resource. Governments are seeking to assert sovereign control over data—like other strategic resources such as land, energy, food, water, and capital[6]—in an emerging era of geopolitical competition.

---

1. *See* VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 78 (2013) ("[Digitization is] the process of converting analog information into the zeros and ones of binary code so computers can handle it. . . . [t]o datafy a phenomenon is to put it in a quantified format so it can be tabulated and analyzed.").

2. On the concept of datafication, see Ulises A. Mejias & Nick Couldry, *Datafication*, 8 INTERNET POL'Y REV., Nov. 29, 2019, at 1–2 (defining datafication as the "quantification of human life through digital information," and thus noting that data increasingly interfaces with human behavior).

3. *See* Ross P. Buckley, Dirk A. Zetzsche, Douglas W. Arner & Brian W. Tang, *Regulating Artificial Intelligence in Finance: Putting the Human in the Loop*, 43 SYDNEY L. REV. 43, 43–44 (2021) (developing a framework to address the AI "black box" problem).

4. The dependence on data is particularly apparent in the context of digital communications, interactions, payments, commerce, and finance. *See generally* Douglas W. Arner, Ross P. Buckley, Andrew M. Dahdal & Dirk A. Zetzsche, *Digital Finance, COVID-19 and Existential Sustainability Crises: Setting the Agenda for the 2020s* (Univ. of N.S.W. L. Rsch. Series, Working Paper No. 003, 2021), http://classic.austlii.edu.au/au/journals/UNSWLRS/2021/16.html (describing the role of the COVID-19 crisis in propelling data aggregation and analytics processes).

5. For an analysis of society's growing dependence on data to perform daily tasks, see LAURA DENARDIS, THE INTERNET IN EVERYTHING: FREEDOM AND SECURITY IN A WORLD WITH NO OFF SWITCH 4 (2020). In the context of medical research and crises response, access to data is essential to ensure innovation and rapid actions. *See* Ciara Staunton, Carlos Andrés Barragán, Stefano Canali, Calvin Ho, Sabina Leonelli, Matthew Mayernik, Barbara Prainsack & Ambroise Wonkham, *Open Science, Data Sharing and Solidarity: Who Benefits?*, 43 HIST. & PHIL. LIFE SCIS. 1, 2 (2021) (noting that one of the fundamental tenets of "open-science" is the possibility of sharing large datasets to promote scientific advancement and solidarity).

6. For comparisons to oil resources, see *Data Is Giving Rise to a New Economy*, THE ECONOMIST (May 6, 2017), https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy ("Data are to this century what oil was to the last one: a driver of growth and change."). For more comparisons, see Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373, 374 (2014); Jakob Svensson & Oriol Poveda Guillén, *What Is Data and What Can It Be Used For? Key Questions in the Age of Burgeoning Data-Essentialism*, 2 J. DIGIT. SOC. RSCH. 65, 66 (2020); Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows* 2 (Org. for Econ. Coop. & Dev., Working Paper No. 220, 2019), https://www.oecd-ilibrary.org/deliver/b2023a47-en.pdf?itemId=%2Fcontent%2Fpaper%2Fb2023a47-en

Through the implementation of new data policies and regulation, general data governance frameworks are emerging, defining a new set of data-related rights and obligations for stakeholders such as data generators and owners. Rooted in different "varieties of capitalism"[7] and modes of regulation,[8] each data governance style[9] reflects the distinct culture, politics, economy, and legal framework applied to data in a given jurisdiction. As analyzed elsewhere, the general data governance styles of the largest economies—the European Union, United States, and People's Republic of China—are colliding, challenging the paradigm of free transnational dataflows and fragmenting the global economy.[10]

Finance is highly dependent on data and its transnational movement. Since the invention of the telegraph in the nineteenth century, finance has grown into the most globalized, digitized, and regulated sector of the modern economy.[11] Underlying this digital transformation, over the past fifty years, financial assets and processes have gradually dematerialized, transforming financial products and information into digital data.[12] Hence, financial entities, consumers, and

&mimeType=pdf; R.J. ANDREWS, INFO WE TRUST: HOW TO INSPIRE THE WORLD WITH DATA 1–40 (2019) (comparing data to water, as it can be stored for later use).

7. *See* Peter A. Hall & David Soskice, *An Introduction to Varieties of Capitalism*, *in* VARIETIES OF CAPITALISM: THE INSTITUTIONAL FOUNDATIONS OF COMPARATIVE ADVANTAGE 1, 8 (Peter A. Hall & David Soskice eds., 2001) (introducing two core types of capitalism—liberal and coordinated—and noting that liberal market economies are more apt to support radical innovation, whereas coordinated market economies tend to support incremental innovation). The notion has been further developed and applied in different contexts. *See, e.g.*, Gregory Shaffer, *Governing the Interface of U.S.-China Trade Relations*, 115 AM. J. INT'L L. 622, 622 (2021) (explaining the different capitalist models between the United States and China in the context of international trade relationships); *see also* Bob Hancké, Martin Rhodes & Mark Thatcher, *Introduction: Beyond Varieties of Capitalism*, *in* BEYOND VARIETIES OF CAPITALISM: CONFLICT, CONTRADICTIONS, AND COMPLEMENTARITIES IN THE EUROPEAN ECONOMY 1, 1 (Bob Hancké et al. eds., 2007) (offering an overview of the application of the varieties of capitalism and a critique in the European context).

8. CARY COGLIANESE & ROBERT A. KAGAN, REGULATION AND REGULATORY PROCESSES xi (Cary Coglianese & Robert A. Kagan eds., 2007) (presenting varieties of capitalism within regulatory processes); Julia Black, *Learning from Regulatory Disasters*, 10 POL'Y Q. 3, 4 (2014) (introducing regulatory governance as a form of managing risks to achieve a publicly stated objective); Giuliano G. Castellano, Alain Jeunemaître & Bettina Lange, *Reforming European Union Financial Regulation: Thinking Through Governance Models*, 23 EUR. BUS. L. REV. 409, 414 (2012) (presenting regulatory models in the European Union).

9. A "data governance style" is a characterization of the overarching approach a jurisdiction takes toward data, data flows, and data infrastructures. *See* Douglas W. Arner, Giuliano G. Castellano & Ēriks K. Selga, *The Transnational Data Governance Problem*, 37 BERKELEY TECH. L.J. 623 (2023) (introducing the notion of "data governance style").

10. *See generally id.* (discussing the evolution of the various regulatory and policy clashes taking place that are inhibiting the free transnational data movement).

11. Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *The Evolution of FinTech: A New Post-Crisis Paradigm?*, 47 GEO. J. INT'L L. 1271, 1274 (2015) (presenting a framework for the globalization of financial transactions enabled by financial technology).

12. Campbell Jones, *The World of Finance*, 44 DIACRITICS 30, 44 (2016) (presenting a case for how the dematerialization of securities has propelled globalization and financialization); Patrice Baubeau, *Dematerialization and the Cashless Society: A Look Backward, a Look Sideward*, *in* THE BOOK OF PAYMENTS 85, 90–91 (Bernardo Batiz-Lazo & Leonidas Efthymiou eds., 2016) (arguing that dematerialization has been fundamental for collateralization, innovation, and inflation); *see* Arner et al., *supra* note 11, at 1279; John O. McGinnis, *The Sharing Economy as an Equalizing Economy*, 94 NOTRE DAME L. REV. 329, 330 (2018) (presenting dematerialization as a wider phenomenon that acts as a force that equalizes access to services, products, and ideas).

regulators routinely share data to provide their services and maintain the stability and integrity of the financial system. Finance's dependence on the flow of data in an environment of growing data regulation raises complex questions regarding how data governance and financial regulation interact, and the implications of that interaction for a digitally globalized financial system.

To tackle these questions, we develop a two-part framework addressing the digitalization of finance. First, we introduce the notion of "financial data governance models." We define financial data governance as an emergent phenomenon, comprising rules, processes, and strategies that shape the legal and regulatory framework pertaining to the digitization and datafication of finance. We posit that these models are influenced by—but sometimes deviate from—the evolution of a jurisdiction's general data governance style.[13] Governance models in China, India, the European Union, and the United States help frame the key components of financial data governance, and their comparison sheds new light on various jurisdictional models. In this context, the relationship between general data governance, financial regulation, and open finance reveals significant interactions.

At its core, financial data governance is comprised of three components: (1) financial regulatory regimes, (2) financial regulatory approaches, and (3) data governance styles. All of these components are specifically applicable to financial data, "the representation of [financial] information, concepts, and other phenomena in different (analog or digital) forms and mediums . . . suitable for communication, interpretation, and processing by human beings or automated systems."[14]

The first component, financial regulatory regimes applicable to financial data, comprises the rules designed to enhance market efficiency; regulate market conduct and fairness; and achieve market integrity, financial stability, and prudential policies.[15] The second component, financial regulatory approaches, focuses specifically on the use of personal financial data and the datafication of finance, such as credit information sharing rules and emerging open banking and open finance strategies, which are designed to facilitate third-party access to

13. *See generally* Arner et al., *supra* note 9.

14. *Id.* at 625 n.1. *See generally* Chaim Zins, *Conceptual Approaches for Defining Data, Information, and Knowledge*, 58 J. AM. SOC'Y FOR INFO. SCI. & TECH. 479 (2007) (exploring the foundations of information science and formulating definitions for data, information, and knowledge). In this Article, we refer to financial data in its digital format.

15. The full suite of financial regulation is applicable to financial data. For a discussion of developments in financial regulation, see generally Christina Parajon Skinner, *Regulating Nonbanks: A Plan for SIFI Lite*, 105 GEO. L.J. 1379 (2017) (describing the architecture of financial regulation in the United States, especially how the Financial Stability Oversight Council supervises nonbank conduct); Lawrence G. Baxter, *Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures*, 66 DUKE L.J. 567 (2016) (discussing how prudential and business supervision is stifled by lack of personal accountability in banking); Lev Menand, *Too Big To Supervise: The Rise of Financial Conglomerates and the Decline of Discretionary Oversight in Banking*, 103 CORNELL L. REV. 1527 (2018) (describing how risk-focused regulation has altered financial supervision).

individual customer financial data held by banks with the consent of the customer.[16] The third component is general data governance styles.[17]

Financial data governance is thus a dynamic phenomenon; its core components interact as different regulatory forces interact. Open finance policies are particularly powerful examples of this dynamic. Open finance is a novel phenomenon that started in the banking sector, where it is referred to as open banking. It allows financial and nonfinancial firms to gain access to the aggregate data of bank customers in order to develop new digital products and services. In the European Union, open banking stems from both the Union's general data governance style, which is aimed at attributing control to individuals over their personal data with consumer protection in view, and specific financial policies concerned with promoting financial inclusion and the creation of a competitive market for financial services. The result is a mandatory regime requiring banks to ensure consent-based access to customer data by third parties. Moreover, while open finance generally dovetails with general data governance frameworks, in some cases, general data regimes may have to adapt to open finance policies. For instance, in the European Union, the individual's right to obtain and reuse their personal data for their own purposes across different services ("data portability") was first introduced in the context of financial regulation, with the Second Payments Directive (PSD2) establishing the requirements of open banking.[18] A year later, the General Data Protection Regulation (GDPR) introduced a general data governance framework extending the concept of data portability beyond the financial domain.[19] Furthermore, the 2020 EU Digital Finance Strategy seeks to expand the scope of the PSD2, creating a broader open finance framework[20] whereby key information collected

16. For more information on open finance, see generally Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 328 (2021) (presenting the concept of "data autonomy" as a measure to introduce open finance in the United States); Germain Bahri & Tabitha Lobo, *The Seven Highly Effective Strategies To Survive in the Open Banking World*, 5 J. DIGIT. BANKING 102 (2020) (presenting several models of open finance, from extending traditional banks into digital banks to providing modular banking services to nonfinancial entities); Linda Jeng, *Inception to Open Banking*, *in* OPEN BANKING 1 (Linda Jeng ed., 2022); Andres Wolberg-Stok, *Open Banking Ecosystem and Infrastructure: Banking on Openness*, *in* OPEN BANKING 13 (Linda Jeng ed., 2022); Douglas W. Arner, Ross P. Buckley & Dirk A. Zetzsche, *Open Banking, Open Data, and Open Finance: Lessons from the European Union*, *in* OPEN BANKING 147 (Linda Jeng ed., 2022); Dan Awrey & Joshua Macey, *The Promise and Perils of Open Finance* (Eur. Corp. Governance Inst., Working Paper No. 632, 2022), https://ecgi.global/sites/default/files/working_papers/documents/maceyawreyfinal.pdf (presenting concentration and other competition risks in open finance).

17. *See supra* note 9 and accompanying text.

18. *See generally* Directive 2015/2366, of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC, 2015 O.J. (L 337) 35.

19. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 89–131.

20. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU*, at 14, COM (2020) 591 final (Sept. 24, 2020).

or produced for public or private use is made available for reuse.[21] In contrast, there is no general legislative framework for personal data in the United States, only for personal data in specific sectors like finance.[22] As a result, open finance is led by industry rather than legislation, and is moving much more slowly.

As financial information is digitized and financial assets move in that direction, finance is becoming inextricably related to data governance. Yet the intersection of financial regulation, new regulatory regimes for digital finance, and general data governance regimes is not always harmonious. Conflicts arising at the intersections of these regimes can frustrate data governance objectives.

Thus, the friction between data governance and jurisdictional financial regulation regimes creates challenges. The concomitant application of general data and financial regulation may generate incongruous outcomes, whereby full access to financial information is limited by data governance regimes. Drawing from the notion of Commercial Law Intersection (CLI),[23] finance-specific regulatory policies and priorities—notably those concerned with market integrity and financial stability—are enmeshed with new data-focused priorities. The aim of these policies and priorities is to allocate control over data while protecting domestic interests. Conflicting priorities between data governance and financial regulation regimes manifest directly in the context of market integrity regulation and addressing criminal and terrorist use of the financial system, commonly referred to as anti-money laundering ("AML"). In a similar vein, conflicting priorities may emerge with personal data privacy regulation—a rapidly increasingly area of regulation.[24] In particular, regulatory conflicts in the European Union over privacy subjects, for example, have resulted in agencies such as Europol having to destroy data on criminal activities or ask suspects' permission to use their data.[25]

---

21. Brett Aho & Roberta Duffield, *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*, 49 ECON. & SOC'Y 187, 199–204 (2020) (outlining how the European Union has adopted consumer- and privacy-protection-oriented regulation to counter growing data-surveillance architecture).

22. *See* sources cited *supra* note 16.

23. The CLI phenomenon is ubiquitous and has been identified in Giuliano G. Castellano & Andrea Tosato, *Commercial Law Intersections*, 72 HASTINGS L.J. 999 (2021) (offering an analytical framework for examining CLI and devising a normative approach to address the issues emerging from the lack of coordination in CLIs).

24. In the European Union, for example, data protection is a protected right under the Charter of Fundamental Rights of the European Union. *See generally* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1727 (2020) (arguing that data protection cannot reach constitutional-level protection in the United States as it does in the European Union); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PENN ST. J.L. & INT'L AFF. 52 (2020) (presenting the bases of privacy in the European Union, China, and United States); Raddivari Revathi, *Evolution of Privacy Jurisprudence – a Critique*, 60 J. INDIAN L. INST. 189 (2018) (presenting privacy law in India).

25. The European Commission and European Data Protection Board (the EU data protection authority) were tasked to clarify "how to reconcile the AML/CFT framework with the applicable data protection legislations," to ensure that data can be shared between obliged entities and competent authorities. Council Conclusions on Anti-Money Laundering and Countering the Financing of Terrorism (EU) No. 12608/20 of 5 Nov. 2020, at 13 [hereinafter Council Conclusions]. This conflict culminated in a recent order from the European Data Protection Supervisor requiring Europol to erase four petabytes of irregularly collected data. *See EDPS*

The international context presents a different set of challenges. Most notably, different regulatory regimes create tensions that threaten the existing paradigm of globalized, free-flowing digital finance. By hindering the ability of financial data to leave jurisdictions, domestic data governance styles also challenge the operational paradigm of the free flow of financial data in global finance. Financial regulation is a highly harmonized architecture of complex soft law, including standard-setting bodies and payment-flow networks.[26] Domestic data governance styles are, by contrast, highly territorialized, leading increasingly to a "splinternet" and "digital Berlin walls."[27] The free movement of financial data across borders is necessary to ensure the stability and integrity of the global financial system, which includes global payment and settlement systems, interbank communication, central banking functions, financial supervision, and international coordination.

Crucially, limited access to data and the absence of mechanisms for sharing financial information among regulators and market participants undermines the ability to price, assess, and monitor risks. This affects financial stability, as both the 1997 Asian financial crisis and the 2008 global financial crisis have demonstrated.[28] When Lehman Brothers failed in 2008, market participants struggled to ascertain their total exposures, given that they were unable to map the nexus of links between different counterparties.[29] No single financial authority could grasp the structure of the global over-the-counter ("OTC")

Decision on the Retention by Europol of Datasets Lacking Data Subject Categorization (Cases 2019-0370 & 2021-0699) 13 (Dec. 21, 2021), https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

26. Lawrence G. Baxter, *Understanding the* Global *in Global Finance and Regulation*, *in* RECONCEPTUALIZING GLOBAL FINANCE AND ITS REGULATION 28, 29 (Ross P. Buckley et al. eds., 2016) (presenting an interconnected soft law network of the G20, Bank for International Settlements, Basel Committee on Banking Supervision, Financial Stability Board, and international financial institutions); Ross P. Buckley, Emilios Avgouleas & Douglas W. Arner, *Three Major Financial Crises: What Have We Learned?*, *in* REGULATION AND THE GLOBAL FINANCIAL CRISIS: IMPACT, REGULATORY RESPONSES, AND BEYOND 19, 19 (Daniel Cash & Robert Goddard eds., 2020) (highlighting that the soft law bodies regulating transnational finance are notably stronger than prior to the crisis, but myopic in their regulatory scope).

27. The idea of a "splinternet" involves reversing the decentralization of internet architecture to allow domestic governments to control and divide internet traffic. *See generally* Mark A. Lemley, *The Splinternet*, 7 DUKE L.J. 1397 (2021); Stacie Hoffmann, Dominique Lazanski & Emily Taylor, *Standardizing the Splinternet: How China's Technical Standards Could Fragment the Internet*, 5 J. CYBER POL'Y 239 (2020) (arguing that the "splinternet" is a result of diverging technical standards in internet infrastructure, which until now has been generally standardized globally); Kristalina Georgieva, Managing Dir., IMF, Keynote Address at the OECD Global Forum on Competition: From Fragmentation to Cooperation: Boosting Competition and Shared Prosperity (Dec. 6, 2021), https://www.imf.org/en/News/Articles/2021/12/06/sp120621-keynote-address-at-the-oecd-global-forum-on-competition (outlining the current trends of technological decoupling and the creation of "digital Berlin walls," with negative impacts for the global GDP).

28. Payal Chadha, *What Caused the Failure of Lehman Brothers? Could It Have Been Prevented? How? Recommendations for Going Forward*, INT'L J. ACCT. RSCH., 2016, at 1 (presenting the lack of monitoring in the financial regulatory framework as a core cause behind the failure of Lehman Brothers).

29. ROSS P. BUCKLEY & DOUGLAS W. ARNER, FROM CRISIS TO CRISIS: THE GLOBAL FINANCIAL SYSTEM AND REGULATORY FAILURE 171 (2011); Richard B. Berner, Robin Doyle & Kenneth Lamar, The Data Reporting Challenge: U.S. Swap Data Reporting and Financial Market Infrastructure (Nov. 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3541248.

derivatives market.[30] More recently, Chinese-based Didi announced plans to withdraw from the New York Stock Exchange, in part due to ongoing regulatory threats from the U.S. government to delist Chinese companies that are not compliant with its auditing rules.[31] This recent example highlights the potential for further fragmentation when financial regulatory requirements (respecting overseas listings), data governance requirements (around national security and the protection of individual data), and emerging financial data governance requirements (in the context of financial data aggregation) do not align. Consequently, the lack of coordination at the transnational level is generating new blind spots in the transnational framework for financial supervision. The systemic implications of these gaps are not fully discernable, but they are reminiscent of the issues that emerged during the 2008 global financial crisis.[32] These issues have received further impetus from the range of financial sanctions placed in the wake of Russia's invasion of Ukraine in February 2022.

The combination of these elements results in composite governance frameworks that, while influenced by broader data policies, are developing independently of one another. For instance, financial data is generally exempted from domestic data-localization rules to avoid blocking global financial flows. More broadly, financial data governance is epitomized by the evolution of open banking in the European Union's PSD2, which requires banks to allow third parties to access customer data with consent,[33] as well as by regulatory regimes addressing credit information reporting[34] and the recent U.S. Anti-Money

30. *See generally* Charles Fergus Graham, *Have EU Derivative Policy Reforms Since the 2008 Financial Crisis Been Designed Effectively?*, 29 J. FIN. REG. & COMPLIANCE 256 (2021); Iman van Lelyveld, The Use of Derivatives Trade Repository Data: Possibilities and Challenges (unpublished manuscript), https://www.bis.org/ifc/publ/ifcb46z.pdf.

31. *See* Scott Murdoch & Sayantani Ghosh, *Analysis: Didi's New York Exit a Further Blow to Chinese Listings in U.S.*, REUTERS, https://www.reuters.com/markets/us/didis-new-york-exit-further-blow-chinese-listings-us-2021-12-03/ (Dec. 5, 2021, 6:12 PM).

32. Several key elements drive these similarities, including regulatory fragmentation tied to lessening global financial information exchange, the development of new opaque financial products and services (like fintech), and increasing complexity in regulating digital financial services. For some examples of these elements in the 2008 global financial crisis, see generally Steven L. Schwarcz & Lucy Chang, *The Custom-to-Failure Cycle*, 62 DUKE L.J. 767 (2012) (providing examples of the elements in the global financial crisis and describing how routine reliance on heuristics in financial regulation can result in regulatory failure and necessitates better regulatory metrics); Iman Anabtawi & Steven L. Schwarcz, *Regulating Systemic Risk: Towards an Analytical Framework*, 86 NOTRE DAME L. REV. 1349 (2011) (discussing the regulatory interventions needed to decrease systemic risk in financial systems from conflicts, complacency, and complexity); Steven L. Schwarcz, *Regulating Shadows: Financial Regulation and Responsibility Failure*, 70 WASH. & LEE L. REV. 1781 (2013) (accounting for a trend of financial services being provided outside the traditional banking system and the emergence of a "responsibility failure" by lack of sufficient government intervention); Kathryn Judge, *Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk*, 64 STAN. L. REV. 657 (2012) (discussing how complexity from financial innovation increases systematic risk).

33. Directive 2015/2366, *supra* note 18.

34. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C. and 20 U.S.C.).

Laundering Act, which established a federally maintained registry where beneficial ownership of legal entities is digitally recorded.[35]

Addressing the incongruencies between jurisdictions' different priorities when it comes to market integrity and financial stability is central to the future of digital dataflows in the global financial system. Different strategies are required to address the tensions in the overlap between data governance generally and financial data governance in particular. Within jurisdictions, the integration between data and financial systems should be seamless, as the digitization and datafication of finance is irreversible. To this end, rules affecting financial data and digital finance should be designed and interpreted to ensure legal coherence in order to redress ambiguities and conflicts in the law.[36]

Transnational fragmentation should be addressed in a different manner. Transnational fragmentation is the result of fundamental differences in strategic policy aims and objectives between jurisdictions, requiring new mechanisms to bridge differences. Unlike transnational data governance,[37] global finance has a well-developed international framework for coordination, standard setting, and information sharing. These frameworks—driven by international cooperation and coordination via the Group of 20, Financial Stability Board (FSB), and a range of other international financial organizations—provide mechanisms for cooperation in many aspects of regulating data in global finance.

Areas of shared concern—including financial stability, financial crime, money laundering, and cybersecurity—will continue to underpin global finance. At the same time, there will be continuing competition to develop financial data governance strategies to maximize domestic gains from the datafication of finance. Central to the future of finance will be the development of coordinated mechanisms where private law, regulations, and technological advances operate harmoniously to address this new reality. For example, the sharing of data by central banks to the Bank for International Settlements is a system that could benefit from legal and technical advances.[38] In addition, emerging

35. Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, 134 Stat. 4547 (codified as amended in scattered sections of 31 U.S.C.).

36. The body of scholarship exploring the notion of coherence is vast. *See generally, e.g.*, Jaap Hage, *Law and Coherence*, 17 RATIO JURIS. 87 (2004); Stefano Bertea, *The Arguments from Coherence: Analysis and Evaluation*, 25 OXFORD J. LEGAL STUD. 369 (2005); Veronica Rodriguez-Blanco, *A Revision of the Constitutive and Epistemic Coherence Theories in Law*, 14 RATIO JURIS. 212 (2001); Aldo Schiavello, *On "Coherence" and "Law": An Analysis of Different Models*, 14 RATIO JURIS. 233 (2001); Aleksander Peczenik, *Law, Morality, Coherence and Truth*, 7 RATIO JURIS. 146 (1994); Joseph Raz, *The Relevance of Coherence*, 72 B.U. L. REV. 273 (1992); S.L. Hurley, *Coherence, Hypothetical Cases, and Precedent*, 10 OXFORD J. LEGAL STUD. 221 (1990); Robert Alexy & Aleksander Peczenik, *The Concept of Coherence and Its Significance for Discursive Rationality*, 3 RATIO JURIS. 130 (1990); Neil MacCormick, *Coherence in Legal Justification*, *in* THEORY OF LEGAL SCIENCE 235 (Aleksander Peczenik et al. eds., 1984); Kenneth J. Kress, *Legal Reasoning and Coherence Theories: Dworkin's Rights Thesis, Retroactivity, and the Linear Order of Decisions*, 72 CALIF. L. REV. 369 (1984); AULIS AARNIO, PHILOSOPHICAL PERSPECTIVES IN JURISPRUDENCE (Ilkka Niiniluoto ed., 1983).

37. *See generally* Arner et al., *supra* note 9.

38. *See generally* IRVING FISHER COMM. ON CENT. BANK STAT., IFC REPORT NO. 1, DATA-SHARING: ISSUES AND GOOD PRACTICES (2015), https://www.bis.org/ifc/events/7ifc-tf-report-datasharing.pdf.

technologies, such as decentralized storage,[39] zero-knowledge protocols,[40] and federated analytics,[41] can help individuals in the industry and regulators store and use data without requiring a transfer across jurisdictional borders. This is a change from the dominant paradigm of the centralization of financial data, epitomized by the U.S. credit information firm Equifax and the theft of essentially all its data on hundreds of millions of U.S. citizens in 2017, to a new paradigm of data decentralization based on new technologies and policy approaches.

This Article is structured in five parts. In Part I, we discuss the digitization of finance and the challenges it poses to traditional financial regulatory objectives: financial stability, consumer protection and fairness, efficiency, and market integrity. We also highlight the evolving nature of finance and the legal and regulatory treatment of data. In Part II, we consider the datafication of finance and the intersection of data, finance, and data governance, highlighting both emerging data governance styles and the evolution of a range of open finance strategies, with a focus on personal financial data. In Part III, we present four emerging financial data governance strategies, exemplified by the United States, European Union, China, and India. These data governance strategies all seek to bring finance and its regulation together with each jurisdiction's evolving domestic data governance regimes. In Part IV, we explain how the differences in these strategies, combined with prudential objectives, result in data territorialization through data localization. We then address this growing challenge of fragmentation in Part V 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 the objectives of both financial and data regulation.

I. THE DIGITALIZATION OF FINANCE

Finance is inextricably linked to the acquisition, analysis, and processing of massive volumes of diverse forms of information. Today, this information is mostly digital. More broadly, financial information—data concerning business and individual transactions—is now the fuel of modern financial systems.

39. Decentralized storage refers to systems with peer-to-peer networks of user operators that hold a portion of the overall data, thus creating a resilient file storage sharing system. *See Decentralized Storage*, ETHEREUM, https://ethereum.org/en/developers/docs/storage/ (Sept. 26, 2022).

40. Zero knowledge protocols are a form of authenticating an entity or certain data without using the information itself to verify its veracity, allowing the communication of information without revealing it to the parties communicating through mathematical models. *See* Lily Hay Newman, *Hacker Lexicon: What Are Zero-Knowledge Proofs?*, WIRED (Sept. 14, 2019, 7:00 AM), https://www.wired.com/story/zero-knowledge-proofs/.

41. Federated analytics allows analyzing data without requiring centralized data collection, ensuring users retain ownership and control over their data while being able to draw on the benefits of aggregated data analysis. *See* Daniel Ramage & Stefano Mazzocchi, *Federated Analytics: Collaborative Data Science Without Data Collection*, GOOGLE AI BLOG (May 27, 2020), http://ai.googleblog.com/2020/05/federated-analytics-collaborative-data.html.

Financial information underlies both the efficient capital markets hypothesis[42] as well as financial regulatory requirements for information disclosure, access, and quality. In addition to investors in stock markets who rely on data analyses to make investment and trading decisions, lenders use data, such as repayment history, credit card transactions, income statements, and asset information, to estimate the credit worthiness of potential borrowers. A wide range of proprietary and shared sources, such as credit-rating agencies, credit bureaus, and social media platforms, compound data and create new hybrid streams of information to analyze. This is exemplified in the rise of fintech and large nonfinancial, data-intensive firms, often called Big Tech.

This Part focuses on the role of digital data in modern finance. First, it demonstrates how the evolution of finance, technology, and related legal schemes has increasingly focused on data. This analysis in turn shows how data is the foundation of modern finance.

A. FINANCE, TECHNOLOGY, AND THE LAW

Finance, technology, and the law developed together, paralleling and interacting with the evolution of civilization.[43] While finance does not produce physical goods, throughout much of human history, it has been supported by physical accounting tools, like papyrus or paper documents, books, coins, or stone tablets. In fact, central to any financial activity is the ability to record transactions and information related to the parties involved; even the simplest moneylender's pawn transaction resulted in a chit for the borrower and a record in the lender's ledger.[44]

> Since the invention of paper in China (2000 years ago) until the late 1970s, finance was an industry based on paper: paper ledgers, paper certificates, and paper money (in addition to coins). With the . . . diffusion of [electronic storage and computing power], finance evolved into a digital industry, where financial instruments (such as stocks and other securities) are [now] dematerialized, and financial information is digital.[45]

---

42. The efficient capital markets hypothesis (also known as the random walk theory) is the proposition that current stock and other publicly available asset prices fully reflect available information about the value of the firm, and there is no way to earn excess profits over the rest of the market by using this information. *See generally* Gili Yen & Cheng-Few Lee, *Efficient Market Hypothesis (EMH): Past, Present and Future*, 11 REV. PAC. BASIN FIN. MKTS. & POL'YS 305 (2008) (surveying the development of the efficient capital markets hypothesis from the 1960s through the 1990s).

43. *See* George Levy, *A Brief History of Finance*, *in* COMPUTATIONAL FINANCE USING C AND C#: DERIVATIVES AND VALUATION 275, 275–99 (2016) (providing a history of finance from ancient to modern times). Finance can be traced back to ancient Sumer, whereby grain and ingots of copper and silver were used as payment. *Id.* at 275. Financial transactions were codified in the Babylonian Code of Hammurabi circa 1800 B.C. *Id.*

44. *See id.* at 275–99.

45. Douglas W. Arner, Giuliano G. Castellano & Ēriks K. Selga, *The Emergence of Financial Data Governance*, OXFORD BUS. L. BLOG (Mar. 29, 2022), https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/03/emergence-financial-data-governance.

The symbiotic relationship between finance and technology is ultimately aimed at supporting the portion of the economy concerned with the production of goods and the provision of services, often referred to as the "real economy."[46] Hence, finance, supported by technology, has developed to allocate and deploy economic resources across industries and market participants.[47] As a result, the financial system has a deep and wide reach, catering to the financing needs of businesses, trades, governments, and individuals.

From the advent of the telegraph in the nineteenth century to the broader integration of information technology in finance in the twentieth century and the fintech movement ushered in the twenty-first century, the local, domestic, and global dimensions of finance have become inextricably intertwined with technological advancement.[48] Today, the global financial system is several times the size of the real economy: the global foreign exchange market turnover is approximately $7.5 trillion each day.[49] This system is almost entirely digital and dematerialized.

Competitive forces underlying financial markets do not always yield desired effects. These malfunctions are commonly referred to as "market failures" and represent one of the primary justifications for regulatory interventions in the financial system.[50] Financial regulation provides a set of rules and principles that instill confidence in the financial system by addressing market failures.

---

46. The term "real economy" refers to that segment of the economic system concerned with the production of goods and supply of services. *See Real Economy*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/real-economy (last visited Jan. 28, 2023).

47. *See* Robert C. Merton & Zvi Bodie, *A Conceptual Framework for Analyzing the Financial Environment*, *in* THE GLOBAL FINANCIAL SYSTEM: A FUNCTIONAL PERSPECTIVE 3 (Dwight B. Crane et al. eds., 1995) (indicating that the overarching socioeconomic function of allocating economic resources across borders and time is realized through a subset of functions, including the clearing and settling of payments, the management of risks, and the deployment of capital).

48. Arner et al., *supra* note 11.

49. *See Triennial Central Bank Survey of Foreign Exchange and Over-the-Counter (OTC) Derivatives Markets in 2022*, BIS (Oct. 27, 2022), https://www.bis.org/statistics/rpfx22.htm. The notional volume of derivatives in 2018 was over $500 trillion—approximately eight times the value of global GDP. *See generally* Servaas Storm, *Financialization and Economic Development: A Debate on the Social Efficiency of Modern Finance*, 49 DEV. & CHANGE 311 (2018) (describing the shift in financial intermediation from banks to financial markets and subsequent growth in rent-seeking practices); Zoltan Pozsar, *Institutional Cash Pools and the Triffin Dilemma of the U.S. Banking System*, 22 FIN. MKTS., INSTS. & INSTRUMENTS 283 (2013) (outlining the rise of a shadow banking system through the avoidance of short-term government guaranteed securities and institutional cash pools).

50. Although other reasons, such as social solidarity, lend strong support to the implementation of regulatory policies, the market-failure rationale—deploying the analytical tools of economics—is considered the main justification for regulating financial markets. *See* JOHN ARMOUR, DAN AWREY, PAUL DAVIES, LUCA ENRIQUES, JEFFREY GORDON, COLIN MAYER & JENNIFER PAYNE, PRINCIPLES OF FINANCIAL REGULATION 51 (2016) (noting that the key features of financial markets make them prone to market failures); Steven L. Schwarcz, *Controlling Financial Chaos: The Power and Limits of Law*, 2012 WIS. L. REV. 815, 818 (arguing that four types of market failures are inherent in the financial system and identifying them as "information failure, rationality failure, principal-agent failure, and incentive failure").

More profoundly, and beyond the traditional market-failure rationale, research indicates that legal and regulatory regimes have evolved with financial markets,[51] demonstrating that finance is a legally constructed phenomenon.[52] The social relationships composing financial markets are embedded in and represented by contractual arrangements, conveying critical financial information. Commercial and financial legal frameworks support the enforceability of obligations contained in such contracts and, together with regulatory regimes, promote certainty in financial transactions, provide essential information necessary for market functioning through disclosure requirements, and instill confidence in the financial systems.[53]

In this context, the law evolves and interacts with the technology underpinning finance. As financial assets, such as securities, are dematerialized and held electronically in depository systems, regulations and private law have had to adapt. The legal status, evidentiary nature, and enforceability of electronic transactions must correspond with the needs of market participants and function at least as well as paper-based transactions. While many of the legal issues concerned with the emergence of electronic financial activities have already been debated and to a large extent addressed,[54] new challenges have emerged as the processes of dematerialization have ushered a more profound, 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.

Three key dynamics are reshaping the financial industry while posing new legal and regulatory challenges and opportunities. First, the emergence and wide diffusion of digital financial services have shifted the focus from digitizing backend processes and activities within financial institutions to deploying technologies delivering financial services to consumers. Second and relatedly, fintech's combination of novel technologies with finance has catalyzed the creation of new business models and products, significantly changing existing

51. Especially important in understanding the evolution of finance and law is the need to go beyond doctrinal analysis to better assess the role of social practices between the two areas. *See generally* Simon Deakin, *The Evolution of Theory and Method in Law and Finance*, *in* THE OXFORD HANDBOOK OF FINANCIAL REGULATION 13 (Niamh Moloney et al. eds., 2015) (expanding on the merits of evolutionary concepts and reasoning to analyze the interrelation of law and finance); Simon Deakin, *The Legal Theory of Finance: Implications for Methodology and Empirical Research*, 41 J. COMPAR. ECON. 338 (2013) (introducing the legal theory of finance as a multidiscipline area of study).

52. *See generally* Katharina Pistor, *A Legal Theory of Finance*, 41 J. COMPAR. ECON. 315 (2013) (arguing that financial markets are legally constructed, and thus law can cause financial markets to collapse); Black, *supra* note 8 (introducing regulatory governance as a form of managing risks to achieve a publicly stated objective).

53. Pistor, *supra* note 52, at 315–17.

54. For an early discussion of the challenges posed by the dematerializations of financial transactions and assets, see generally Chris Reed, *The Law of Unintended Consequences – Embedded Business Models in IT Regulation*, J. INFO., L. & TECH., Nov. 2007, https://warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/reed/ (discussing how IT-aware regulation will struggle to catch up with technological developments and leave outlying risks in the process); CHRIS REED, ELECTRONIC FINANCE LAW (1991) (providing a systematic overview of the dematerialization of finance).

financial practices. Third, the increasing integration of novel technologies has allowed for the diffusion of digital finance and the advancement of fintech solutions. New forms of digital assets based on distributed ledger technology (DLT) such as blockchain; new forms of analytics such as artificial intelligence (AI), machine learning, and Big Data; and new forms of data storage and communication including cloud and the Internet of Things are transforming finance.

The digitalization of finance has also resulted in the creation of new financial-inclusion policies[55] through digital financial services ranging from mobile payments to larger platform-based ecosystems using consumer-generated data to tailor financial products. In fact, digital solutions are instrumental to broadening access to financial services and catering to the financing needs of individuals and small businesses.

To unlock the potential of digital finance, regulatory policies have focused 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 and other finance initiatives, whereby payment and banking service providers are encouraged to allow authorized third-party access to customer and payment accounts information.[56] While complying with this core objective, financial institutions and jurisdictions can adopt a variety of approaches, like selecting the level of openness or type of services and integrating their offerings with the business models of other players.[57] The result is a financial system where financial data becomes a resource expanding the reach of financial services, and a commodity that can be integrated into new financial services.

55. *See generally* Douglas W. Arner, Ross P. Buckley, Dirk A. Zetzsche & Robin Veidt, *Sustainability, FinTech and Financial Inclusion*, 21 EUR. BUS. ORG. L. REV. 7 (2020) (highlighting how digital finance has been used to address both micro and macroeconomic challenges related to sustainability); Majid Bazarbash, *FinTech in Financial Inclusion: Machine Learning Applications in Assessing Credit Risk* 2 (IMF, Working Paper No. WP/19/109, 2019), https://www.imf.org/-/media/Files/Publications/WP/2019/WPIEA2019109.ashx (discussing how novel technological capabilities like machine learning help encourage financial inclusion).

56. See *infra* Part III.D. for a more in-depth discussion of open finance.

57. For an overview of different business strategies, see generally Bahri & Lobo, *supra* note 16.

B. THE DIGITIZATION OF FINANCE AND THE PERVASIVENESS OF FINANCIAL DATA

Financial data is a broad, but distinct, form of data. It includes traditional banking data, transactions history, and other information typically tied to individual accounts and users. Such data is used for various purposes, including the assessment of various risks, based on models calculating the probability of repayment and the pricing of different services. Financial data also includes data about financial markets and products such as stock prices and the accounting data of 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 terrorism ("AML/CFT") as part of market-integrity regulation,[58] and market, client, statistical, and transaction data are used to determine the level of protection (particularly in the context of capital and liquidity levels) against various prudential risks, including credit, market, and operational risk.[59]

Financial data thus is not an autonomous legal category, as it overlaps with a variety of different classifications pertaining to the general governance framework. It includes nonpersonal data concerning clients and transactions that are collected to send instructions for payments, report to regulators, and offer financial services. It also includes personal data tied to individuals, such as individual account information on individual transactions, and other sensitive information.

The breadth, depth, and importance of financial data 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 and sufficiently prescriptive for use by regulators and policymakers, while affording sufficient protection to the growing amounts of personal and public data. The intersection of policy aims is best exemplified through the emergence of open finance, an initiative involving all three core actors: the public sector, the market, and the individual.

58. For example, customer due diligence requirements necessitate the collection of a variety of personal information from customers of financial institutions to ensure the source of funds is of licit origin.

59. For discussions exemplifying regulatory reporting requirements for financial data, see generally Abdullahi Usman Bello & Jackie Harvey, *From a Risk-Based to an Uncertainty-Based Approach to Anti-Money Laundering Compliance*, 30 SEC. J. 24 (2017); Patrik Alamaki & Daniel Broby, The Effectiveness of Regulatory Reporting by Banking Institutions (2019) (unpublished manuscript) (on file with the Centre for Financial Regulation and & Innovation).

C. THE DATAFICATION OF FINANCE: FINANCE AS DATA

The coalescence of finance and data has changed the nature of financial activities.[60] While the relationships between finance and data are partially shaped by the financial system, they are also shaped by forces outside the traditional boundaries of the financial industry.[61] Big Tech, for example, is quickly acquiring the capacity to offer advanced financial services, competing with traditional finance providers like banks and investment companies.[62] These dynamics mark an evolutionary step toward the integration of data and financial systems.[63]

Furthermore, the novel use of growing amounts of accessible financial and other data, together with new technology, are extending the frontiers of financial services. For instance, the availability of large amounts of data is fueling a diffused deployment of AI in retail,[64] professional trading,[65] compliance, and regulation.[66] Moreover, the ability to ensure data integrity in a decentralized fashion through DLT is prompting profound transformations in supply-chain financing as well as the development of new classes of assets. In a similar vein, the emergence of cryptocurrencies, digital assets, and decentralized finance (DeFi) is also encouraging the decentralization of data and data-related services, with the promise of creating a new financial infrastructure.[67]

In this environment, data is not just a vehicle of financial information; it is a constitutive component of finance. Finance is largely data. Datafication spurs

60. For an overview of how finance is being changed by digitalization, see generally Dirk A. Zetsche, William A. Birdthistle, Douglas W. Arner & Ross P. Buckley, *Digital Finance Platforms: Toward a New Regulatory Paradigm*, 23 U. PA. J. BUS. L. 273 (2020) (regarding the platformization of finance); Arner et al., *supra* note 9; Helen Bollaert, Florencio Lopez-de-Silanes & Armin Schwienbacher, *Fintech and Access to Finance*, J. CORP. FIN., June 2021 (discussing lending, crowdfunding, and initial coin offerings).

61. Zetsche et al., *supra* note 60; Arner et al., *supra* note 11; Bollaert et al., *supra* note 60.

62. *See generally, e.g.*, Lianrui Jia & Dwayne Winseck, *The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization*, 80 INT'L COMM'N GAZETTE 30 (2018) (describing financialization as to the growth of the financial sector and of BAT in China).

63. Arner et al., *supra* note 11, at 1273.

64. AI for retail is exemplified by its use in predictive recommendations for product offerings and predictive pricing for insurance services. *See generally* Peter K. Yu, *Artificial Intelligence, the Law-Machine Interface, and Fair Use Automation*, 72 ALA. L. REV. 187 (2020) (discussing the challenges arising from the confluence of human and machine-hybrid decisionmaking systems, including in the optimization of retail products like insurance).

65. AI for professional trading utilizes hundreds of thousands of data points to capture real-time information and conduct automated transactions. *See generally* Ariel Fzrachi & Maurice E. Stucke, *Sustainable and Unchallenged Algorithmic Tacit Collusion*, 17 NW. J. TECH. & INTELL. PROP. 217 (2020) (highlighting that algorithmic trading utilizing artificial intelligence is creating new tacit collusion risks).

66. Compliance AI is exemplified by dynamic and automated client risk assessment for banks, which draws on a variety of traditional and alternative data to conduct iterative analysis. William Magnuson, *Artificial Financial Intelligence*, 10 HARV. BUS. L. REV. 337 (2020) (arguing that the growing dependence on AI in financial intelligence will bolster human error and detailing how AI is being deployed to combat money laundering through automating customer due diligence).

67. *See generally* Linn Anker-Sørensen & Dirk Andreas Zetzsche, *From Centralized to Decentralized Finance: The Issue of "Fake-DeFi"* (Eur. Banking Inst., Working Paper No. 97, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3978815 (describing DeFi and highlighting the trend of false decentralization).

the acquisition and analysis of new digital data that, in turn, enables the development of new technological solutions. For example, by deconstructing financial services into their constituent data parts, financial services are becoming increasingly modular, allowing their separation into multiple backend and frontend services that can work independently to create a seamless banking experience for customers. The datafication of finance promotes the ever-growing financialization of the modern economy, as financial transactions connect market participants around the world and data is traded within and outside the financial system.[68] Financial instruments, payment systems, trading venues, and compliance functions are part of an ecosystem where data is a representation of information about market participants and transactions, as well as the main asset traded itself. The result is an industry where trillions of dollars are traded every day in a nonphysical manner through a digital infrastructure with a global reach.[69]

II. FINANCIAL DATA GOVERNANCE: REGULATING THE DIGITIZATION AND DATAFICATION OF FINANCE

Financial data governance encompasses a variety of rules and principles that can be grouped into three categories. The first category comprises rules regulating the production, acquisition, use, and circulation of financial data. These rules are central to 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 evolve with digitalization and technological advancement. 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, dataflows, and infrastructure. These emerged initially in the context of personal data, but are now being extended to national security, competition, and developmental objectives. The third category comprises the emerging regulatory initiatives, strategies, and models for digital finance, such as open banking and open finance policies focusing on personal financial data that have developed to address challenges and opportunities caused by the digital transformation of the financial sector. The coalescence of a diverse range of traditional and novel regulatory regimes concerned with financial data and the datafication of finance is creating a new governance framework for digital finance.

This Part considers the evolution of the key components of financial data governance. First, it examines the regimes regulating the digitization of financial

68. Storm, *supra* note 49, at 314 (arguing that the "financialization of everything" has facilitated rent-seeking practices).

69. *Id.* at 317.

information. Then, it considers the development of open banking and open finance and how they work in different jurisdictions.[70]

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 relates to the digitization of finance. Financial regulation has adapted to ensure that the risks related to the growing reliance on digital information, financial assets, and related infrastructures are properly addressed. Gathering, processing, managing, and using digital financial information has become central to financial regulatory policies concerned with the solvency of financial institutions and the stability and 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.

With respect to prudential policies, since the year 2000 or "Y2K," and after the 9/11 attacks in 2001, regulators have focused on the risks emerging from the growing integration of digital systems in financial activities. Technological failures, cyberattacks, legal actions, and regulatory sanctions related to the mistreatment of data are a form of operational risk that impact the solvency of financial institutions. As data and technology are inextricably related to finance, new international standards have developed to ensure that technology-related operational risks are properly addressed. For example, 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 principled approach to strengthen operational resilience within banks.[71]

From a conduct of business standpoint, the three primary regulatory concerns over the treatment of financial data relate to the promotion of market integrity, market efficiency, and investor and consumer protection.

---

70. The development of different jurisdictional data governance styles has been discussed extensively elsewhere and will not be restated here. *See generally* Arner et al., *supra* note 9.

71. Capital requirements for operational risks are enshrined in the Consolidated Basel Framework; with the new rules, the ability of banks to use their own estimations to assess capital requirements is limited. *See* BANK FOR INT'L SETTLEMENTS, CONSULTATIVE DOCUMENT: CONSOLIDATED BASEL FRAMEWORK 1, 4, 7–8 (2019), https://www.bis.org/bcbs/publ/d462.pdf. In addition, with the last revision of the Principles for Operational Resilience, the BCBS updated its guidance on operational risk to include information and communication technology risks, including cybersecurity, and to also require the sound structuring of data, especially regarding third-party service providers. *See* BANK FOR INT'L SETTLEMENTS, REVISIONS TO THE PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK 15–16 (2021), https://www.bis.org/bcbs/publ/d515.pdf.

In the context of market integrity, AML requirements mandate financial service providers to integrate many categories of data into their risk calculations in transactions involving different products, clients, or geographies. Information on markets and customers is essential for financial institutions to determine their risk exposure.[72] Here, for example, personal data (i.e., information concerning transactions or bank accounts) is collected to feed into suspicious transaction reporting, informing financial intelligence units and relevant supervisory agencies.

From a market failure standpoint, a central focus of regulation is on the quality and availability of information. Disclosure requirements, such as those enforced by the U.S. Securities and Exchange Commission, and information quality assurance regulations of gatekeepers, such as accountants, auditors, intermediaries, credit-rating agencies, and credit bureaus, constitute a large portion of financial regulation and are central to market functioning, investor protection, and market participant decisionmaking.

Lastly, many broader regulatory reporting requirements depend on financial data. Regulators are requiring banking data to be machine-readable to enable supervisory automation processes and more granular data-aggregation capabilities.[73] 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.[74] Regulatory and supervisory technology models ("RegTech" and "SupTech") are requiring financial data to be structured so that regulators have direct access through automatically packaged business data (data-input approach), collecting business data directly from bank systems (data-pull approach), or analyzing operational bank data at will (real-time access). These RegTech and SupTech technologies are not only expanding the micro-prudential supervisory capacity, but are also enabling the aggregation of vast data pools for machine-learning and AI solutions used for risk management.

The second dynamic affecting the regulation of financial data involves the interaction between financial regulatory regimes and general data policies. As data is treated as a strategic resource and governance expands its

72. The process of assessing risk for the application of regulatory standards is also known as the "risk-based approach." FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH - THE BANKING SECTOR 4 (2014) (providing an overview of the main international principles governing the risk-based approach in the context of AML requirements).

73. FIN. STABILITY BD., THE USE OF SUPERVISORY AND REGULATORY TECHNOLOGY BY AUTHORITIES AND REGULATED INSTITUTIONS: MARKET DEVELOPMENTS AND FINANCIAL STABILITY IMPLICATIONS 1, 32 (2020), https://www.fsb.org/wp-content/uploads/P091020.pdf (discussing the drivers, benefits, and challenges of SupTech and RegTech).

74. TORONTO CTR., FINTECH, REGTECH AND SUPTECH: WHAT THEY MEAN FOR FINANCIAL SUPERVISION 11 (2017) (presenting the range of utility of RegTech and SupTech, including the novel data analytic uses they open).

reach domestically and internationally,[75] regulatory regimes concerned with the treatment of financial information naturally intersect and interact with general data policies. In fact, financial data encompasses multiple classes and types of data that, while used for financial purposes, may also fall squarely into general data categories, particularly personal data. Consequently, the holders and processors of financial data are increasingly regulated, directly or indirectly, by general data governance rules in force in any given jurisdiction. These general regimes typically establish rights concerned with the alienability, circulation, or management of personal financial data.[76] However, at the same time, financial data (personal and nonpersonal) is also the object of specific regulatory initiatives that stem from sector-specific needs and concerns.

B. REGULATING THE DATAFICATION OF FINANCE AND THE EMERGENCE OF OPEN BANKING AND OPEN FINANCE

Financial data is impacted directly by both financial regulation and general data governance styles. Financial regulation and general data governance styles, both within and across jurisdictions, frequently overlap and conflict.

For instance, unlike the European Union, which has had a formal legal framework for personal data since 1995,[77] the United States has not had a general legislative framework governing personal data. Instead, the United States has a complex array of federal and state laws that regulate personal data. In 2018, California adopted the first comprehensive state data protection legislation, the California Consumer Privacy Act (CCPA), which became effective in 2020.[78] However, outside of data regulation, the United States has enacted federal legislation in a number of finance-specific areas. The most significant are the Fair Credit Reporting Act, enacted in 1970[79] and amended by the Fair and Accurate Credit Transactions Act of 2003,[80] and the Gramm-Leach-Bliley Act,[81] which created the Consumer Financial Protection Bureau (CFPB),[82] which regulates consumer financial data. Absent a general

75. The treatment of data as a strategic resource manifests especially in regard to critical infrastructure and functions like national security, financial markets, and transportation. *See generally* Arner et al., *supra* note 9.

76. See *infra* Part IV for a discussion of regulatory fragmentation and data territorialization caused by the emergence of data governance styles. *See generally* Arner et al., *supra* note 11.

77. *The History of the General Data Protection Regulation*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Jan. 28, 2023) (describing the development of data protection in the European Union).

78. California Consumer Privacy Act of 2018, Ch. 55, 2018 Cal. Stat. 1807 (codified as amended at CAL. CIV. CODE §§ 1798.100–.199.100 (West 2020)).

79. Pub. L. No. 91-508, tit. VI, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. § 1681 *et seq.*).

80. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended in scattered sections of 15 U.S.C. and 20 U.S.C.).

81. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

82. Jolina C. Cuaresma, *Commissioning the Consumer Financial Protection Bureau*, 31 LOY. CONSUMER L. REV. 426, 428–30 (2019) (discussing the unique leadership and accountability structure of the Consumer Financial Protection Bureau).

data protection framework, these Acts can be seen as sector-specific elements of the United States' general data governance style, which may eventually form the basis of a broader set of rules governing personal data in the United States.

In contrast, the European Union has long had a general framework for personal data protection, although prior to 2018 this framework had a limited impact on financial data. This changed, however, with the implementation of both PSD2 and GDPR in 2018.[83] 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 European Union's general data governance style and its financial data governance strategy.

Not only does open banking parallel and interact with the European Union's general data governance style, but it is also emerging as a separate yet related regulatory strategy. The European Union is the first mover and leading proponent of a mandatory legislative approach toward financial data governance that reflects and extends its more general data governance style. In the European Union, PSD2 (which predates GDPR) established a framework promoting novel payment service providers through a licensing structure requiring banks to provide third-party access to a client's payment account with the client's consent.[84] Banks have to comply with a system of data-transferring rules by developing application programming interfaces (APIs) that meet a minimum set of functional standards.[85] PSD2, however, only mandates sharing by banks, an aspect that it has been criticized for.[86]

The open banking and open finance movement is spreading globally, albeit in differing forms. To unlock the potential of the digital economy, jurisdictions are pursuing a range of open finance variants.

At the most basic level, open finance enables consumer-generated data to be transferred (data portability) or accessed by third parties. Open banking typically limits sharing to banks, while open finance encompasses the full range of financial services providers, ranging from banks and other traditional

83. Dirk A. Zetzsche, Douglas W. Arner, Ross P. Buckley & Rolf H. Weber, *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II* 6, 14–15, 22, 24–25 (Eur. Banking Inst., Working Paper No. 35, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359399.

84. Markos Zachariadis, *How "Open" Is the Future of Banking? Data Sharing and Open Data Frameworks in Financial Services*, *in* THE TECHNOLOGICAL REVOLUTION IN FINANCIAL SERVICES: HOW BANKS, FINTECHS, AND CUSTOMERS WIN TOGETHER 129, 142–43 (Michael R. King & Richard W. Nesbitt eds., 2020) (explaining that PSD2 creates a tripartite system where account-servicing payment service providers (ASPSPs) like banks must share their data securely with authorized third-party providers that are either account information service providers (AISPs) that provide consolidated information on a user's payment accounts or payment initiation service providers (PISPs) that offer an online service to initiate payment orders requested by users).

85. Crucially, banks must (1) allow AISPs and PISPs to identify themselves to the bank; (2) permit AISPs and PISPs to communicate securely in order to request and receive accounts and payment information; and (3) allow PISPs to initiate payment orders from customer payment accounts, as well as to receive the necessary information regarding the initiation and execution of said payment transactions. *See* Regulation 2016/679, *supra* note 19.

86. Arner et al., *supra* note 16, at 4–5, 12, 18.

intermediaries to fintech and Big Tech. Approaches can range from legislatively mandated approaches (as in the European Union) to industry-led voluntary systems approaches (as in the United States), with a range of roles for regulators in between.[87] In mandatory systems like the European Union, Australia, and the United Kingdom, core provisions have been adopted. These provisions mandate financial institutions to grant third-party access to data, regulate access through APIs, and establish standardized digital IDs for users.

Comparing different rules offers a useful illustration of how policymakers in different jurisdictions understand and promote open banking or open finance. Open banking or open finance in one jurisdiction can be very different from open banking or open finance in another, particularly in the legal bases underlying open banking and open finance policies and those policies' interaction with general data governance styles.

Data portability lies at the heart of open finance strategies. The main difference between jurisdictions is in the degree of requisite data portability. For instance, while U.S. federal law does not require data portability, the CCPA gives users the right to receive their personal information in a useable, readable format for easy transmission from their data holder to other entities.[88] Thus, the open finance strategy in the United States is voluntary, and one which so far has largely been ineffectual as a result of industry recalcitrance. The European Union's 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 from the rest of their data.

The approach adopted to foster open finance in any given jurisdiction is an important proxy for gauging the trajectory of that jurisdiction's financial data governance. Generally, open finance policies aim to regulate the relationships between (i) financial data holders, such as banks and other financial institutions; (ii) processors, such as technology-focused fintech firms; and (iii) users, mostly represented by individuals and small business.[89]

These actors can be further divided into subcategories. Banks and other financial institutions can be aggregators that combine services from third-party providers to enhance their offerings or provide new services. Financial institutions can also be distributors, giving third-party processors access to clients' data. This is evident, for instance, in the context of stockbroker functions, which banks commonly outsource to third parties while seamlessly integrating them into their customer interface. Other financial institutions can also offer data-orchestration services by, for instance, bringing together data

87. *See generally id.*

88. CAL. CIV. CODE §§ 1798.110(b), 1798.130(a)(3)(B)(iii) (West 2020).

89. These are the core stakeholders in the open finance cycle, consisting of entities that generate, process, and hold data. *See* Yan Carrière-Swallow, Vikram Haksar & Manasa Patnam, *India's Approach to Open Banking: Some Implications for Financial Inclusion* 4, 22–23 (IMF, Working Paper No. WP/21/52, 2021), https://www.imf.org/-/media/Files/Publications/WP/2021/English/wpiea2021052-print-pdf.ashx.

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 policies in the European Union, the policies in the United Kingdom and Australia[90] are seen as strong examples of legislatively mandated open banking and open finance strategies, while the policies in the United States are seen as an example of an industry-led, voluntary open finance strategy. In between these extremes lie a range of models, usually characterized by the level of regulatory guidance and involvement. For example, the strategies in Singapore and Hong Kong are both characterized by active guidance from regulators through standard setting, but both lack legislative mandates. Singapore, in particular, has been very active in building an infrastructure and implementing regulatory guidance through guidelines and nonbinding documents. This guidance serves as the basis of its open finance strategy, which suggests that the regulator-led approach is another possible data governance style.

China is also developing its own variant of open finance. In China, much of the consumer-authorized financial data access takes place 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 an internal enterprise and external APIs instead of just focusing on bank-to-customer interactions. The 2018 guidelines for data governance established detailed structures for the data management of financial institutions.[91] A more recent set of interim provisions stipulate minimum consent and require that consent be requested before giving third parties access to financial data.[92] It is becoming a mandatory system, albeit with data as a publicly shared resource rather than one controlled by individuals or financial institutions.

Likewise, India is developing another open finance strategy, one based on individual control of data—as in the European Union, United Kingdom, and Australia—but with its use facilitated through a system of licensed data

90. Ross P. Buckley, Natalia Jevglevskaja & Scott Farrell, *Australia's Data-Sharing Regime: Six Lessons for Europe*, 33 KING'S L.J. 61, 90 (2022).

91. *Zhongguo Yinhang Baoxian Jiandu Guanli Weiyuanhui Fabu《Yinxingye Jinrong Jigou Shuju Zhili Zhiyin》* (*中国银行保险监督管理委员会发布《银行业金融机构数据治理指引》*) [*China Banking and Insurance Regulatory Commission Issued the "Guidelines for Data Governance of Banking Financial Institutions"*], GUANGDONGSHENG DIFANG JINRONG JIANDU GUANLI JU (广东省地方金融监督管理局) [GUANGDONG FIN. SUPERVISORY AUTH.] (May 22, 2018, 00:00 AM), http://gdjr.gd.gov.cn/gdjr/jrzx/jryw/content/post_2870321.html.

92. *《Yidong Hulianwang Yingyong Chengxu Geren Xinxi Baohu Guanli Zanxing Guiding》Gongkai Zhengqiu Yijian* (*《移动互联网应用程序个人信息保护管理暂行规定》公开征求意见*) [*"Interim Provisions on the Protection and Management of Personal Information of Mobile Internet Applications" for Public Comments*], ZHONGHUA RENMIN GONGHEGUO GUOJIA HULIANWANG XINXI BANGONGSHI (中华人民共和国国家互联网信息办公室) [CYBERSPACE ADMIN. OF CHINA], http://www.cac.gov.cn/2021-04/26/c_1621018189707703.html (announcing the "Interim Provisions on the Protection and Management of Personal Information of Mobile Internet Applications" by the Cyberspace Administration of China).

aggregators known as the India Stack.[93] Firms licensed by the Reserve Bank of India act as fiduciaries, collecting customers' financial data and sharing it with customers' consent to third parties.[94] Following the objectives of financial inclusion and facilitating financial competition in the market, account aggregators are a public good that ensure a level playing field, precluding the accrual and appropriation of data-management costs by individual institutions while allowing reciprocal data sharing.[95] Through aggregate banking, the goal is to extend the India Stack from payments into credit, personal finance, wealth management, and insurance.

Thus, jurisdictions are developing a variety of strategies to create open finance systems—each designed to maximize the benefits of personal financial data—bridging financial regulation and general data governance styles, and often modifying both.

III. EMERGING FINANCIAL DATA GOVERNANCE STRATEGIES

General data governance styles interact with financial regulation in the financial data governance model of any given jurisdiction. Each data governance style leaves a footprint on the financial data governance model of the jurisdiction. Each footprint reflects different degrees of control over data handed to one category of societal actors populating the data ecosystem. What or who controls data in general, and financial data more specifically, is dependent on what a jurisdiction prioritizes. A jurisdiction may prioritize (i) market dynamics, where data holders, such as business organizations and financial institutions, are key players; or (ii) the interests of individuals, primarily as the data generators; or (iii) the public interest, represented by state actors and public entities.

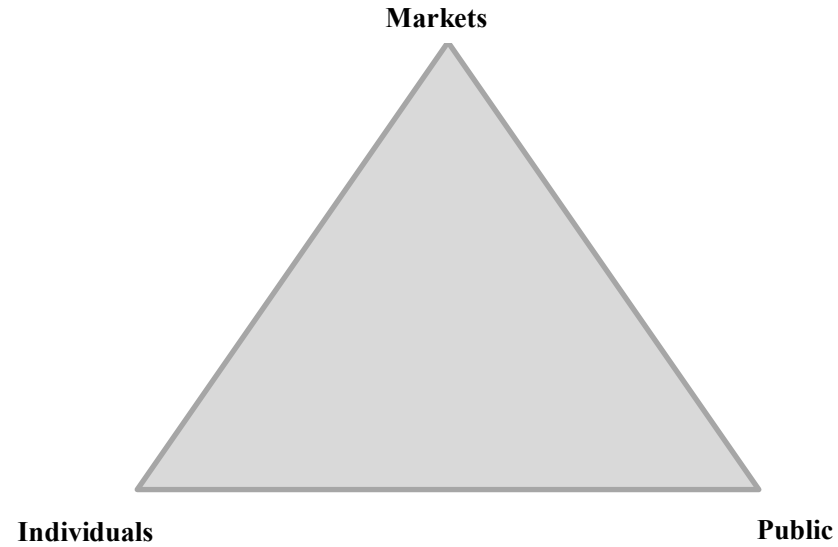
Through this prism, we identify three data governance model archetypes. In market-focused models, jurisdictions allow market dynamics to control data. Hence, public policies are primarily designed to protect the emergence of a market for data; regulatory interventions are limited to the correction of market failures and to the protection of critical domestic interests, such as national security. In individual rights–focused models, jurisdictions allow the individuals generating such data to control it. From a policy standpoint, protection for consumers and data generators tends to be preferred over market dynamics, prompting the adoption of regulatory intervention to curb excessive private power. Finally, in public-focused models, data is conceived as a collective resource. Jurisdictions with this data governance style typically have a public authority governing the gathering and use of data through rules that leave limited room for interpretation when market participants apply them.

93. Shri M. Rajeshwar Rao, Deputy Governor, Rsrv. Bank of India, Speech at Reserve Bank of India (Apr. 14, 2021); *see also* INDIA STACK, https://indiastack.org/ (last visited Jan. 28, 2023).

94. Nandan Nilekani, *Data to the People: India's Inclusive Internet*, 97 FOREIGN AFF. 19, 25–26 (2018).

95. Carrière-Swallow et al., *supra* note 89, at 22.

FIGURE 1: DATA CONTROL CONCENTRATION TRIANGLE



These archetypes extend to financial data governance. The different levels of control over data attributed to societal actors influences how financial data is regulated and intersects with open finance policies. These three models are analyzed next. First, the market-based model is analyzed, which represents the status quo: favoring the development of the data economy and the internet. The analysis then moves to the individual rights–based and public-centered models, which largely developed to curb the excessive concentration of power accumulated by private entities, primarily those based in the United States and in China. Examples of all three archetypes are examined through the regulatory policies adopted in China, the European Union, the United States, and India, which represents a hybrid model.

A. MARKET-BASED MODELS

Central to a market-oriented financial data governance model is the notion that data is an asset that can be produced, priced, and exchanged.[96] Essentially, data is addressed as property that is freely alienable.[97] Regulatory interventions are limited and intended to promote confidence in the market while

96. In order to provide financial services, relational data on how certain assets change in ownership or status must be accessible to providers. *See generally* Salome Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573 (2021) (presenting how different jurisdictions are treating data as alienable and "propertarian" or as a reflection of selfhood and "dignitarian").

97. *Id.*

protecting the integrity and stability of the financial system.[98] Access to and transfer of data are contractual matters, left to the free negotiation between parties.[99] Rights over the use of data concerning accounts, payments, and transactions are retained by financial institutions.[100] Data generators, however, may be granted a right to data portability and can request third-party access.

This approach is epitomized by the data governance style adopted in the United States, where the market-based approach has supported 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 users' inputs and outputs in their bank without drawing on the data from the bank's servers.[101] The consensus is that direct access to data through APIs is superior to screen scraping by way of security, reliability, and user control.[102] With screen scraping, there are no binding policies that address the issues of informed consumer consent, the scope and duration of access to data, and the allocation of liability in case of data loss or misuse.[103]

The industry takes the lead in establishing standards for open finance products and services. The Clearing House, a banking association responsible for payment system infrastructure in the United States,[104] has proposed a model agreement standard for data sharing between financial service providers. The aim is to transition from screen scraping to APIs. A more technical set of standards has already been established by the Financial Data Exchange, a cross-section of banks, data aggregators, and technology companies created in 2018.[105] These standards create an interoperable API for user-permissioned financial

98. *See generally* Saule T. Omarova, *Dealing with Disruption: Emerging Approaches to Fintech Regulation*, 61 WASH. U. J.L. & POL'Y 25 (2020) (discussing how even in emerging financial technology, the regulatory trend is still to "experiment," "accommodate," and "incorporate" novelties, rather than challenge them).

99. *See generally* Natalie M. Banta, *Property Interests in Digital Assets: The Rise of Digital Feudalism*, 38 CARDOZO L. REV. 1099 (2017) (arguing against owners' broad freedom to privately contract to utilize their data and that such contracts are disproportionately powerful devices for the control of data).

100. *See generally* Benjamin Wong, *Confidential Information and Data Protection*, 21 SAL ANN. REV. 291 (2020) (analyzing several cases where courts have found that organizations have a right to utilize client data for preservation of evidence, movement between subsidiary data intermediaries, and other aspects as long as there is advanced notice and consent).

101. *See generally* Han-Wei Liu, *Two Decades of Laws and Practice Around Screen Scraping in the Common Law World and Its Open Banking Watershed Moment*, 30 WASH. INT'L L.J. 28 (2020) (arguing that screen scraping may be a more sticky regime in the United States compared to open banking, which requires a lot of institutional collaboration).

102. *Id.*

103. *Id.* at 30.

104. The Clearing House is owned by the largest banks of the United States and has a daily clearing and settlement volume of $2 trillion. *See Model Agreement*, THE CLEARING HOUSE, https://www.theclearinghouse.org/connected-banking/model-agreement (last visited Jan. 28, 2023).

105. *About FDX: Our Mission*, FIN. DATA EXCH., https://www.financialdataexchange.org/FDX/FDX/About/About-FDX.aspx?hkey=dffb9a93-fc7d-4f65-840c-f2cfbe7fe8a6 (last visited Jan. 28, 2023).

data, sharing over 600 types of financial information, including banking, tax, insurance, and investment operations.[106]

While the United States is the clearest example of a market-based model for financial data governance, in reality, financial regulation in the United States—as highlighted in Part II—has long addressed consumer protection in the context of financial data. Thus, the United States can be considered the leading example of a market-based general data governance. In the context of financial data governance, however, it has developed a range of personal and other financial data rules designed to support market efficiency, consumer protection, and financial stability.

More recently, consumer financial data protections embedded in the Fair Credit Act have been extended. The strategic role of data and the emergence of new risks for consumers and the financial sector at large pushed the adoption of new rules to facilitate data access and use. For instance, in October 2020, the CFPB issued an advance notice of proposed rulemaking under section 1033 of the Dodd-Frank Act.[107] Section 1033 requires covered providers of consumer financial services to make consumers' data available to them in a usable electronic format and empowers the CFPB to issue rules.[108] The Dodd-Frank Act's definition of "consumer" is not limited to individuals and includes representatives acting on an individual's behalf.[109] The advance notice of proposed rulemaking, however, only outlined principles for safeguarding consumer interests without setting any standards that consumer financial service providers must follow. Hence, though industry standards like The Clearing House's model agreement aim to incorporate principles from the notice of proposed rulemaking, they remain nonbinding.[110] On this basis, we term the overarching approach to open finance in the United States "contract banking," wherein the level of third-party access an individual can offer to their account information depends in large part on the bilateral agreement between the individual and financial service provider.[111]

106. FIN. DATA EXCH., https://financialdataexchange.org/FDX/Home/FDX/Default.aspx?hkey=bd839735-ebf5-426a-91f9-8334cbae1438 (last visited Jan. 28, 2023); Tom Carpenter, *The State of Open Banking and Open Finance in the US and Canada – Interview with FDX (Part 1)*, THE PAYPERS (Jan. 7, 2022), https://thepaypers.com/interviews/the-state-of-open-banking-and-open-finance-in-the-us-and-canada-interview-with-fdx-part-1—1253761.

107. *Consumer Financial Protection Bureau Releases Advance Notice of Proposed Rulemaking on Consumer Access to Financial Records*, CONSUMER FIN. PROT. BUREAU (Oct. 22, 2020), https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/.

108. Pub. L. No. 111-203, § 1033, 124 Stat. 2008 (2010) (codified at 12 U.S.C. § 5533).

109. *Id.* § 1002(4) (codified at 12 U.S.C. § 5481(4)).

110. *Value and Benefit of Model Data Access Agreement*, THE CLEARING HOUSE 1–2, https://www.theclearinghouse.org/-/media/new/tch/documents/data-privacy/model-agreement-companion-document-final.pdf (last visited Jan. 28, 2023).

111. The "contractual" relationship between individuals and financial service entities in the United States has been discussed elsewhere. *See generally* Bridget A. Fahey, *Data Federalism*, 135 HARV. L. REV. 1007

The Biden Administration has questioned the contract banking standard. Until recently, U.S. laws governing data collection and use focused almost exclusively on protecting consumers from harm caused by unauthorized access to and inappropriate uses of their data. President Biden's recent executive order directs the CFPB to finalize policy work to ensure that consumers and small businesses can "more easily switch financial institutions and use new, innovative financial products."[112] While no new rules have been announced by the CFPB, a first step will involve clarifying the Dodd-Frank Act's establishment of a direct financial data access right for consumers, including authorized data access for third parties chosen by the consumer.

The challenge for the United States will be whether its sector-based approach to data access and use will prove effective. Much depends on how data is perceived at the federal level, where the complex system of informal and formal rules on public dataflows remains largely unregulated.[113]

B. INDIVIDUAL RIGHTS–BASED MODELS

An individual rights–based model for financial data governance prioritizes individuals' control over market dynamics. Data is treated as an individual right rather than as freely alienable property. The gathering, use, and transfer of data are regulated through statutory rights that apply to contractual negotiation and limit both the transferability of data ownership and private entities' control over data. Separation of personal and nonpersonal data is key, as more restrictions are applied to the former, which encompasses information deemed sensitive. Nonpersonal data is generally treated as alienable property.

This model is epitomized by the approach adopted in the European Union. The general data governance framework of the European Union has evolved around three core priorities: (i) a focus on individual rights and privacy, (ii) the prevention of data concentration in a handful of dominant firms, and, more recently, (iii) developing sufficient technological capacity to promote the growth of the European economy. Starting with a series of data protection and privacy directives focused on protecting consumers, the data governance framework has expanded in scope and influence.[114] Most recently, both GDPR and PSD2 adopted a series of measures granting ownership and control of data to individuals.[115] The trajectory is poised to be reinforced with the EU-wide digital

(2022) (presenting the exchange of data between public entities in the United States as horizontally contractual, rather than in a top-down organized flow).

112. Exec. Order No. 14,036, 86 Fed. Reg. 36,987, 36,998 (July 9, 2021).

113. Fahey, *supra* note 111 (presenting a case for the structure underlying data pools in U.S. intergovernmental data exchange).

114. Thomas Streinz, *The Evolution of European Data Law*, *in* THE EVOLUTION OF EU LAW 902, 905–10, 933–36 (Paul Craig & Gráinne de Búrca eds., 2021).

115. Article 36 of the PSD2 requires member states to "ensure that payment institutions have access to credit institutions' payment accounts services . . . [and] to allow payment institutions to provide payment services in an unhindered and efficient manner," thus implicitly requiring data control on behalf of bank clients. *See*

ID regime through the eIDAS regulation, which establishes a framework for digital access to cross-border public and private services in the European market.

In the European Union's data governance style, different regulatory regimes apply to nonpersonal and personal data. Nonpersonal data is generally alienable and can circulate freely.[116] Domestic authorities must be able to access certain data, even if it is in different member states. Accordingly, data holders must implement measures to facilitate data portability between service providers.[117] A different regime applies to personal data, which is inalienable from the individual it pertains to, regardless of any contractual agreement.[118] The GDPR allows personal data to be exported after the recipient has been certified by the European Commission.[119] This certification requires that the regulatory framework of the recipient non-EU jurisdiction ensures basic protections deemed equal to those applied in the European Union.[120] Furthermore, member states can "enact data localization measures, in the context of health, financial services, or other sectors."[121]

Granting control over data to individuals is a pillar of this system. In the open banking strategy, individuals maintain control over their data, and financial institutions can share data with authorized third parties only if it is requested by customers.[122] Yet financial institutions must also ensure that the transfer of data can occur in a systematized fashion and in compliance with a set of minimum requirements.[123]

Building on this framework, the 2020 EU Digital Finance Strategy (DFS) aims to create a single digital market for financial service providers to boost

---

Directive 2015/2366, *supra* note 18, art. 36. Article 20 of the GDPR provides the right of data subjects to "receive the personal data concerning [them]" from data controllers. *See* Regulation 2016/679, *supra* note 19, art. 20.

116. Article 4 of Regulation 2018/1807 prohibits "[d]ata localisation requirements," thus requiring the free flow of data in the EU. Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303) 59, 66.

117. 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." *Id.* art. 5. Such requests can in practice require real-time access and data localization. *See id.* Article 6 encourages the development of "principles of transparency and interoperability" to facilitate switching service providers and the porting of data. *Id.* art. 6.

118. Article 17 of Regulation 2016/679 grants the "right to be forgotten" by allowing users to, with certain limitations, require that data controllers erase personal data concerning them when the data are no longer necessary. Regulation 2016/679, *supra* note 19, art. 17.

119. *Id.*

120. *Id.*

121. Arner et al., *supra* note 9, at 649; Regulation 2016/679, *supra* note 19, art. 17; *see* NIGEL CORY, ROBERT D. ATKINSON & DANIEL CASTRO, PRINCIPLES AND POLICIES FOR "DATA FREE FLOW WITH TRUST" 1, 2–3 (2019), https://www2.itif.org/2019-principles-policies.pdf (highlighting the limits of data protection under GDPR); *see also generally* NIGEL CORY, CROSS-BORDER DATA FLOWS: WHERE ARE THE BARRIERS, AND WHAT DO THEY COST? (2017), https://www2.itif.org/2017-cross-border-data-flows.pdf (highlighting the transaction costs of data protection regimes).

122. 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." Directive 2015/2366, *supra* note 18, art. 64.

123. For example, Articles 65 through 72 of Directive 2015/2366 set out a variety of procedural rules on initiating a payment on behalf of a client via a third-party service provider. *See id.* arts. 65–72.

scalability and competition.[124] This strategy includes enabling interoperable EU-wide use of digital identity documents to allow easier onboarding (initial registration of users) and the "reuse" of onboarding for other purposes beyond financial services (like registration for public services). This data space is centered on a new EU digital finance platform that enables industry and supervisory authorities to interact online, offering e-licensing procedures to expand onboarding regimes and data exchange.[125] 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 "open data," in which data is fully under individual control with the necessary standards and infrastructure to enable use.[126]

The challenge will likely not be the legal framework, because it is relatively simple to qualify data as a right subject to individual control from a legal standpoint. It is much more difficult to build the necessary technological infrastructure that enables individuals to have actual control over their data and sharing it, which is the ideal of open finance and open data. While a range of jurisdictions are following the European Union's legal approach, the biggest challenge for most jurisdictions is building the necessary technological infrastructure to make it actually work in practice. The European Union will likely make this happen, particularly in the context of finance, through the creation of industry-wide data pools and mandatory data-sharing regimes, as we discuss in Part V.

C. PUBLIC-FOCUSED MODELS

In jurisdictions adopting a public-focused 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 through direct public interventions. These protections include minimum rights that protect users (data generators), while public authorities control data, dataflow, and data infrastructures.

China is the emblematic example of a jurisdiction implementing a public-focused model. Characterized by a state-centric structure, China's system supports growth of its internal data market, which benefits the national

124. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data*, at 4–5, 25, COM (2020) 66 final (Feb. 19, 2020) [hereinafter *Communication from the Commission*]; REINER SCHULZE & DIRK STAUDENMAYER, EU DIGITAL LAW: ARTICLE-BY-ARTICLE COMMENTARY 2 (2020); Despoina Anagnostopoulou, *The EU Digital Single Market and the Platform Economy*, *in* ECONOMIC GROWTH IN THE EUROPEAN UNION: ANALYZING SME AND INVESTMENT POLICIES 43, 45, 50, 53 (Christos Nikas ed., 2020); LUÍS CABRAL, JUSTUS HAUCAP, GEOFFREY PARKER, GEORGIOS PETROPOULOS, TOMMASO VALLETTI & MARSHALL VAN ALSTYNE, THE EU DIGITAL MARKETS ACT: A REPORT FROM A PANEL OF ECONOMIC EXPERTS 1, 6–7, 9–10 (2021), https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122910/jrc122910_external_study_report_-_the_eu_digital_markets_acts.pdf.

125. CABRAL ET AL., *supra* note 124, at 4.

126. *See generally Communication from the Commission*, *supra* note 124.

collective. The overarching developmental goal exemplified by China's data governance style is enshrined in the notion of "Common Prosperity."[127] Data governance policy under the Common Prosperity agenda forms a public-focused model that pursues two objectives. First, the data governance policy is intended to achieve social, economic, and financial stability while maintaining national security.[128] Second, data policies aim to bolster competition to promote innovation through the development of an internal digital market.[129]

These two objectives have resulted in public-private relationships that evolved codependently. Prior to 2020, data in China (and the rest of the world) was treated in a way that was functionally similar to the United States' approach. In this paradigm, a small number of large firms gathered and traded data on consumers' behavior.[130] Over time, regulators, through a series of legislative and policy interventions, began to centralize control over data to curb excessive accumulation of power in private hands.[131] Furthermore, "over the past decade, the domestic market was largely protected from foreign competition."[132] This combination of factors led to the development of national champions such as Alibaba, Weibo, Baidu, and QQ; technical mechanisms to block data inflows and outflows; and institutional capacity for the central government to monitor a vast amount of data.[133] This policy led to a flourishing data economy, and as of 2020, the data circulating domestically in China amounts to almost a third of the global movement of data.[134]

In the past few years, a "cyber sovereignty" framework has developed that promotes innovation while keeping data under state control. The central pillars of this framework are three fundamental laws: the 2017 Cybersecurity Law, 2021 Data Security Law, and 2021 Personal Information Protection Law,

127. Zhonghua Renmin Gongheguo Guomin Jingji He Shehui Fazhan Di Shisi Ge Wu Nian Guihua He 2035 Nian Yuanjing Mubiao Gangyao (中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要) [Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035] (promulgated by Nat'l People's Cong., March 12, 2021, effective March 12, 2021) art. 2, § 2, art. 17, § 2 [https://perma.cc/73AK-BUW2], *translated at* https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

128. *See generally* Rogier Creemers, *China's Conception of Cyber Sovereignty: Rhetoric and Realization*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY (Dennis Broeders & Bibi van den Berg eds., 2020) (discussing the overarching goals of Chinese data governance policy).

129. *Id.*

130. *Id.*

131. Together, the 2017 Cybersecurity law, 2021 Data Security Law, and 2021 Personal Information Protection Law limit private company dominance over data. *See* Arner et al., *supra* note 9, at 631.

132. *Id.*

133. China blocks access to ten of the top twenty-five top global websites, creating a parallel internet for dominant websites in China to flourish. *See* Sebastian Hermes, Eric Clemons, Maximilian Schreieck, Simon Pfab, Maya Mitre, Markus Böhm, Manuel Wiesche & Helmut Krcmar, *Breeding Grounds of Digital Platforms: Exploring the Sources of American Platform Domination, China's Platform Self-Sufficiency, and Europe's Platform Gap* 4–5 (Eur. Conf. on Info. Sys., Research Paper No. 132, 2020), https://aisel.aisnet.org/ecis2020_rp/132/ (discussing the access dynamic between online platforms around the world).

134. *See* Aho & Duffield, *supra* note 21, at 188; *see also generally* 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 (2021) (discussing the size of China's state-centric form of capitalism).

reflected in a new State Council policy framework enacted in August 2021.[135] While control over data under the emerging system follows an individual rights–based model like the one deployed in the European Union—whereby personal data is inalienable and nonpersonal data can be freely disposed—the central government ultimately controls data. Not only does the government have access to data, but it also mandates data collection and analysis in both the public and private sector, with a focus on enhancing the Social Credit Score, a local government and private sector system that records the activities of individuals using their Chinese digital identities in online services.[136] This Social Credit Score is a central mechanism for monitoring data. Moreover, although the government allows data to flow uninhibited "internally, data can only leave or enter China with express government permission."[137]

This state-based data governance style extends to a shared banking paradigm. The style is reflected most directly in the banking context, with a series of regulatory interventions triggered by concerns about the Chinese fintech giant Ant Financial.[138] These interventions led to a series of regulatory changes targeting Ant Financial and others, with some interventions increasing government access to data gathered by Ant Financial, and others introducing stringent cybersecurity requirements more generally.[139]

Financial data is thus increasingly treated as a public resource that is under the control of the central government. The largest Chinese digital platforms and Big Tech firms are entrusted to gather data that feeds into users' social credit scores. Data is also fed into commercial and financial scoring systems that are both public and proprietary. Additionally, data generated from dispute resolution cases, contract fulfilment, and other financial activities are gathered and used to help determine these various credit scores.[140] WeChat, an omnichannel platform owned by Tencent with one billion active users, feeds the information back to the Chinese government upon request so that the government can build personalized emotional, behavioral, and physiological datasets and add this information to users' health portfolios.[141] Similarly, Chinese authorities have

135. *Zhonggong Zhongyang Guowuyuan Yinfa《Fazhi Zhengfu Jianshe Shishi Gangyao (2021–2025 Nian)》(中共中央国务院印发《法治政府建设实施纲要 (2021–2025 年)》)* [*The Central Committee of the Communist Party of China and the State Council Issued the "Implementation Outline for the Construction of a Government Ruled by Law (2021–2025)"*], Xinhuawang (新华网) [Xinhuanet] (Aug. 11, 2011, 7:35 PM), http://xinhuanet.com/2021-08/11/c_1127752490.htm.

136. *See* Arner et al., *supra* note 9, at 658.

137. *Id. See generally* Angela Huyue Zhang, *Agility over Stability: China's Great Reversal in Regulating the Platform Economy*, 63 HARV. INT'L L.J. 457 (2022) (highlighting China's expanding regulatory oversight through antitrust, financial, and data regulation). *See* Hermes et al., *supra* note 133, at 4–5.

138. *See* Zhang, *supra* note 137, at 458–62.

139. *Id.*

140. Lizhi Liu & Barry R. Weingast, *Taobao, Federalism, and the Emergence of Law, Chinese Style*, 102 MINN. L. REV. 1563, 1587–88 (2018).

141. 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, 23 (2020); Lizhi Liu, *The Rise of Data Politics: Digital China and the World*, 56 STUD. COMP. INT'L DEV. 45, 48 (2021); Quan Li, Lan Lan, Nianyin

provided express lists of essential and nonessential data that financial service providers can request from users.[142]

More profoundly, in a recent regulatory intervention, the People's Bank of China and other financial supervisory authorities ordered thirteen of the largest technology firms to unbundle and restructure their businesses in order to separate internet-based activities from financial activities.[143] A license is required to separate these types of data.[144] As a result, financial services, which originally developed to support the data economy, are controlled by the government to "break [the] information monopoly" and "enhance the sense of social responsibility."[145]

Thus, China is taking a very different avenue than the United States or European Union, although all three seek to address similar concerns around financial stability, consumer protection, national security, competition, and innovation.

D. HYBRID MODELS

Jurisdictions' approaches to data governance can be categorized depending on whether they prioritize market dynamics, individual rights, or public interests, resulting in archetypical data governance models. Although jurisdictions may favor a certain model, often a jurisdiction's data governance model attempts to balance the three. 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 to one of the three main social groups. Hybrid archetypes emerge when a model does not distinctly prioritize one of the three social groups.

A leading example of the hybrid model is India. The Indian data governance approach is a hybrid model that prioritizes granting individuals and the state control over data. At the heart of this model is a balancing act between

Zeng, Lei You, Jin Yin, Xiaobo Zhou & Qun Meng, *A Framework for Big Data Governance to Advance RHINs: A Case Study of China*, 7 IEEE ACCESS 50330, 50330–31 (2019); Lulu Yilun Chen, *China Considers Creating State-Backed Company To Oversee Tech Data*, BLOOMBERG, https://www.bloomberg.com/news/articles/2021-03-24/china-is-said-to-mull-state-backed-company-to-oversee-tech-data (Mar. 24, 2021, 6:26 PM).

142. *China Seeks To Rein in Mobile Apps' Collection of Personal Data*, REUTERS (Mar. 22, 2021, 12:29 AM), https://www.reuters.com/technology/china-seeks-rein-mobile-apps-collection-personal-data-2021-03-22/.

143. Press Release, The People's Bank of China, Financial Regulators Have Joint Regulatory Talk with Internet Platform Enterprises Engaged in Financial Businesses (May 2, 2021), http://www.pbc.gov.cn/en/3688110/3688172/4157443/4244296/index.html (including thirteen firms: 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).

144. *Id.*

145. *Id.*

the digitalization of financial and public services, the maintenance of a rights-based system for data, and the need to promote competitive market dynamics.[146]

The public sector approach is exemplified by the "India Stack." The India Stack is a multilayered digital infrastructure that India has introduced over the past ten years. The India Stack is underpinned by a strategy to develop infrastructure that enables wider development, innovation, and digitalization across the country. It consists of a range of APIs, open standards, and infrastructure standards and systems that allow Indian citizens to access a broad range of digital services.[147] Since 2011, over ninety percent of the Indian population has received a digital identity, and more than half of the identity holders have linked their bank accounts to their digital identities.[148]

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.[149] The second layer consists of the Unified Payments Interface, an API-based interoperable payments interface that can be used by banks and vendors to send money between financial service providers.[150] 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.[151] The last layer is the consent layer, which enables the active management of individuals' data through regulated intermediaries. For instance, the government has established a voluntary, standard consent template that enterprises must use to replace opaque and unclear terms and conditions.[152] The aim of Aadhaar has been primarily to bring India's residents online to ensure financial inclusion and access to public services, with an emerging secondary goal of benefitting market actors.[153]

The second aim in India's data governance style is oriented at market actors. India Stack's financial inclusion ethos dovetails with the objective of promoting competition within the domestic financial sector.[154] The Indian financial landscape is dominated by state-owned banks that hold almost two-thirds of India's total banking assets.[155] By increasing ease of access to

146. NANDAN NILEKANI, IMAGINING INDIA: THE IDEA OF A RENEWED NATION 42 (1st ed. 2009) (arguing that IT infrastructure has been one of the main enablers of Indian economic growth).

147. Carrière-Swallow et al., *supra* note 89, at 4–5 (describing the development of the India Stack and noting the upcoming "consent layer" as a further enabler of financial data governance).

148. *Id.*

149. *Id.* at 6.

150. *Id.* at 20.

151. *Id.* at 8, 16.

152. Nilekani, *supra* note 94, at 25.

153. Carrière-Swallow et al., *supra* note 89, at 4.

154. RSRV. BANK OF INDIA, NATIONAL STRATEGY FOR FINANCIAL INCLUSION 2019-2024, at 6 (2019).

155. *Id.*

financial services—especially in cashless format—competition within its banking sector is expected to increase.[156]

India has a competitive financial market composed of domestic and foreign-invested firms, including telecoms, payments, ecommerce, fintech, and a range of financial incumbents.[157] Hence, in a way that is akin to a market-based model, these companies all benefit from the India Stack while competing for users. Moreover, the recently adopted Information Technology Rules increase the accountability of social media platforms and empower their users through a redressal mechanism requiring a procedure for reporting and removing content.[158] The appointed grievance officer must acknowledge user complaints within twenty-four hours and resolve disputes within fifteen days;[159] complaints about content containing nudity, sexual acts, or impersonation must be removed immediately.

The trend toward market dynamics is also reflected in India's open finance strategy. The strategy is centered around account aggregators, whereby financial institutions are required to collect data and share it with third parties. In this context, financial institutions act as fiduciaries that source data,[160] but may not access, store, or further sell the acquired data.[161] Account aggregators authenticate users using their Aadhaar IDs and then map the IDs to available documents in the third layer of the India Stack, which gains access to users' information and retrieves their financial assets, liabilities, or cashflows.[162] This system enables broader financial service origination, underwriting, disbursement, and payments.[163]

Through account aggregators, India is seeking to provide an interoperable data standard. The system allows data sharing of more classes of data than other jurisdictions, lending availability to any data held in the India Stack. The broader aggregate-banking approach extends beyond the relationship between financial

156. Carrière-Swallow et al., *supra* note 89, at 20.

157. In 2020, the government of India banned the use of 118 Chinese mobile apps over reports of "stealing and surreptitiously transmitting users' data in an unauthorized manner to servers which have locations outside India." Press Release, Ministry of Elecs. & IT, Government Blocks 118 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order (Sept. 2, 2020), https://pib.gov.in/PressReleasePage.aspx?PRID=1650669.

158. Ministry of Elecs. & IT, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*, PRS LEGIS. RSCH. (Feb. 25, 2021), https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021.

159. *Id.*

160. Account aggregators are defined under section 3 of the Reserve Bank of India Act as "non-banking financial compan[ies] . . . that undertake[] the business of an account aggregator [providing under a contract, the service of, retrieving or collecting information of its customer pertaining to such financial assets, as may be specified by the Bank from time to time; and consolidating, organizing and presenting such information to the customer or any other person as per the instructions of the customer], for a fee or otherwise." *See* Reserve Bank of India, Master Directions on Relief/Savings Bonds, RBI/DNBR/2016-17/46 § 3(1)(i) (Issued on Sept. 2, 2016).

161. *Id.* § 3(1)(iv).

162. *Id.*

163. *What Is the India Stack? Nandan Nilekani Explains*, DIGFIN (July 28, 2020), https://www.digfingroup.com/what-is-india-stack/.

services providers and natural persons, as the India Stack data is also used by and for legal persons. However, the data-aggregators system has not been extended to other areas like search and social media businesses.[164]

The resulting hybrid model reflects strong state control over data infrastructure for broader economic, financial, and developmental purposes, emphasizing a market and public sector focus. Yet individuals are also significantly protected in the Indian system. For example, the powers of state actors are curtailed by the Indian constitutional framework and a personal data bill expected to be enacted in the near future.[165] In this context, the Indian Supreme Court decided that Aadhaar identities can be required to receive welfare benefits,[166] while also finding that mandatory linking of Aadhaar accounts is generally unconstitutional, with limited exceptions.[167] Banks, for instance, are not allowed to deny service if the customer has no linked Aadhaar number.[168] This dynamic epitomizes how the Indian approach strives to balance the pursuit of public policy and the protection of individual rights. The result is a hybrid approach to financial data governance: 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 Big Tech firms).

164. Carrière-Swallow et al., *supra* note 89, at 21.

165. Alpha Partners, *India: Update on Data Protection Law*, MONDAQ (Jan. 3, 2022), https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law.

166. Utkarsh 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 (Jan. 21, 2021, 6:16 AM).

167. Ananya Bhattacharya, *Aadhaar Is Voluntary—but Millions of Indians Are Already Trapped*, QUARTZ INDIA, https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/ (July 20, 2022).

168. *Id.*

TABLE 1: FINANCIAL DATA GOVERNANCE MODELS

Models	Jurisdiction	Open Finance Type	Participation	Digital-ID Scheme	API Standardization	Data-Sharing Reciprocity
Market	United States	Data portability	Voluntary (upon request of customers)	No	No	Voluntary
Individual	European Union	Regulated open banking	Mandatory	Partly; eIDAS-based	Yes	Asymmetric; banks required to share
State	China	Centralized, shared data	Mandatory	Yes	No	Voluntary
Hybrid	India	Aggregate, platform-based	Mandatory	Yes	Yes	Banks, nonbanks may participate voluntarily

Authors' research.[169]

The emergence of financial data governance models depicts a global regulatory landscape where the international flow of financial information is challenged by local regimes. Similar to the observations advanced in the context of the global data economy, where data governance styles are limiting the free circulation of data,[170] financial data governance models are disrupting the process of global integration among financial information networks that started in the 1970s.[171] This trend is particularly evident when certain financial data is categorized as "personal data" under domestic laws.

IV. CHALLENGING THE GLOBALIZATION OF FINANCE

The intersection between data, finance, private law, and regulation is not always harmonious. Finance is one of the most highly regulated industries, with complex networks of soft and hard rules addressing financial stability, market integrity, market efficiency, and consumer protection.[172] This makes international financial policy coordination difficult, especially with the addition of a new layer of data governance. Overarching policy objectives are set by the Group of 20, and standards are set by transnational regulatory bodies like the BCBS and the FSB, but these standards differ significantly in domestic-level

169. For an analysis of the variables in the table, see generally Arner et al., *supra* note 9; Carrière-Swallow et al., *supra* note 89.

170. See *supra* Part II.B for a discussion of localization and other trends related to data governance styles.

171. See *supra* Part I for a discussion of the evolution of digital and globalized finance.

172. DOUGLAS W. ARNER, FINANCIAL STABILITY, ECONOMIC GROWTH, AND THE ROLE OF LAW 154 (2007).

implementation.[173] While the regulatory framework for financial data and the emergence of open finance initiatives can coexist with financial regulatory policies, domestic data governance styles aimed at asserting jurisdictional sovereignty over data, its flows, and its infrastructure create new, and at times incongruous, regulatory challenges.

This Part examines three areas of financial data governance where such challenges are clearest. First, we highlight regulatory fragmentation—the growing divergence of data governance styles—and the need for coordination when financial data falls concomitantly under the authority of different legal and regulatory branches.[174] Second, we discuss territorialization and data localization where jurisdictions create mandatory requirements to collect, process, and store data within their territorial boundaries.[175] The growing emphasis on data localization—while intended to enhance *domestic* financial stability—may in fact harm *global* financial stability. As global markets and risks transcend domestic boundaries, data localization can hamper international coordination to maintain global financial stability. Similarly, geopolitical and competition issues are increasingly impacting financial data governance and the globalization of digital finance. Third, we argue that data localization leads to a fragmentation of financial data and regulatory regimes within and across countries. The result is regulatory arbitrage whereby financial institutions avoid regulatory requirements, as thorough compliance can be monitored globally only if data can circulate freely.

A. REGULATORY FRAGMENTATION

To examine the regulatory fragmentation of financial data governance approaches, we draw from and expand upon the theory of CLI.[176] Data governance rules do not pertain strictly to commercial law, or to financial regulation more specifically.[177] Generally, data governance includes a variety of rules and regulatory regimes that, depending on the jurisdiction's domestic data

173. The policy direction of financial regulation is established primarily within the Group of Seven (G7) and the Group of Twenty (G20), the seven and twenty most industrialized nations, respectively. *See* Shawn Donnelly, *Financial Stability Board (FSB), Bank for International Settlements (BIS) and Financial Market Regulation Bodies*, *in* RESEARCH HANDBOOK ON THE EUROPEAN UNION AND INTERNATIONAL ORGANIZATIONS 360, 360, 384 (Ramses A. Wessel & Jed Odermatt eds., 2019) (describing the role of the G7 and G20 in setting core policy directions for international organizations, and discussing how other organizations like the European Union participate in the process). The direction established in these fora sets the policy parameters for transnational regulatory bodies. *See id.* at 361.

174. *See generally* Arner et al., *supra* note 9.

175. *Id.*

176. The CLI phenomenon is ubiquitous and has been identified in Giuliano G. Castellano & Andrea Tosato, *Commercial Law Intersections*, 72 HASTINGS L.J. 999 (2021) (offering an analytical framework to examine CLI and devising a normative approach to address the issues emerging from the lack of coordination in CLIs).

177. In American legal scholarship, commercial law is traditionally understood as "the body of rules regulating commerce," which includes "the law[s] governing individuals engaged in the manufacture and distribution of objects" as well as "the laws regulating the association of capital." Layton B. Register, *The Dual System of Civil and Commercial Law*, 61 U. PA. L. REV. 240, 241, 243–44 (1913).

governance style, cover how data is created, classified, collected, processed, and used for the purpose of reaching specific policy aims.[178] Yet the convergence of these regulatory regimes in the emerging area of financial data governance creates issues similar to those observed in the CLI context. There, multiple legal rules apply concomitantly, and the lack of coordination between the rules causes tensions or "coordination failures."[179]

In the context of financial data governance, coordination failures can take place on two different levels. On the first level, there can be coordination failures between the policy objectives of financial and data regulation, generally.[180] This is to say that at least one of the policy aims of data regulation, such as cybersecurity or individual privacy,[181] is at odds (or largely incompatible) with one or more of the policy objectives of financial regulation, such as financial stability, market fairness or efficiency, and consumer protection.[182] The second level of coordination failure, while not involving policy objectives, involves conflicts between dispositive rules and principles,[183] such as rules establishing the non-alienability of personal data or operative prepositions. Operative prepositions are the rules and principles that fall within legal doctrines[184] such

178. See *supra* Part II.B for a discussion of localization and other trends related to data governance styles.

179. Scholars have repeatedly emphasized the need for better coordination between branches of commercial law; corporate law, securities regulation, accounting, and others have complicated and sometimes conflicting rules. *See generally, e.g.*, Catherine Walsh, *The Role of Party Autonomy in Determining the Third-Party Effects of Assignments: Of "Secret Laws" and "Secret Liens*," 81 L. & CONTEMP. PROBS. 181 (2018) (emphasizing the need for coordination across commercial branches to expand access to credit); Giuliano G. Castellano & Marek Dubovec, *Global Regulatory Standards and Secured Transactions Law Reforms: At the Crossroad Between Access to Credit and Financial Stability*, 41 FORDHAM INT'L L.J. 531 (2018) (focusing on the intersection between secured transactions law and prudential regulation); Lawrence A. Cunningham, *A Prescription To Retire the Rhetoric of "Principles-Based Systems" in Corporate Law, Securities Regulation, and Accounting*, 60 VAND. L. REV. 1409 (2007) (denouncing the complexities of the intersections of corporate law, securities regulation, and accounting). International organizations have likewise indicated coordination issues as problematic. *See, e.g.*, U.N. COMM. ON INT'L TRADE L., DRAFT LEGISLATIVE GUIDE ON SECURED TRANSACTIONS, at 31, U.N. Sales No. E.09.V.12 (2019) (indicating that the applicability of secured transactions law in a given legal system might be restricted by other laws).

180. Policy aims set the priorities and shape the development of each branch of law. These policy aims are extrapolated from a range of diverse sources including statutes, regulatory principles, or case law. *See* Castellano & Tosato, *supra* note 23, at 1021.

181. 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 European Union, the respect for private family life and protection of personal data are fundamental rights enshrined in the European Charter of Fundamental Rights. *See* Charter of Fundamental Rights of the European Union, art. 7, 2000 O.J. (C 364) 1, 10. Discussions on the interpretation of data privacy are also seeing growing academic discussion. *See, e.g.*, Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721, 2722 (2021) (arguing in favor of deleveraging the use of the Stored Communications Act to bar subpoenaing the contents of one's online communication in a criminal defense).

182. This is considered a "multi-core CLI coordination failure"—one which is characterized by gaps or incongruences that stem from the tension between the core spheres of two or more of the converging legal branches. *See* Castellano & Tosato, *supra* note 23, at 1047.

183. This is considered a "different-sphere failure," characterized by gaps or incongruencies stemming from tensions between different aspects of multiple branches of law. *See id.*

184. "Operative propositions" indicate the rules and principles that fall within the system of legal doctrines underlying key tenets of a law branch. *See id.* at 1045.

as the specific rules regulating APIs or the format and modes in which customer data must be collected.[185]

The frictions between privacy objectives, prudential rules, efficiency, and transparency of payment systems are an example of the first level of coordination failure. With cash payments, there is inherently full privacy because cash-based transactions are anonymous. However, this degree of anonymity, which is a rich ground for money laundering activities, is not a feature of DLT payments.[186] For central bank digital currencies (CBDCs), anonymity, at least vis-à-vis regulators and enforcement authorities, is not an option; however, privacy protection is critical in many jurisdictions.[187] As a public good, privacy is important for a variety of reasons, such as preventing data-based price discrimination[188] and ensuring democratic functions.[189] For this reason, jurisdictions have considered different forms of privacy measures, including regulatory techniques like government access to data that is based solely on the issuance of a warrant and cryptographic methods that automate pseudo-anonymization.[190]

Nonetheless, each option requires a compromise or tradeoff between policy objectives.[191] Prioritizing privacy objectives necessarily results in the subordination of financial regulation policies that are aimed at ensuring the integrity, fairness, and efficiency of financial markets. In a similar vein, pursuing financial regulation policies that are solely focused on integrity, fairness, and efficiency of financial markets leads to less privacy protections. The inability to collect, process, or exchange an individual's transaction or other financial data between financial entities can, for example, skew their risk-assessment capacity, potentially compounding the risks they take. This tradeoff will likely result in a range of different structures within new digital monetary initiatives such as CBDCs that reflect jurisdictions' differing balances of social objectives.

AML most directly exemplifies the coordination failure between data governance (data privacy and use) and financial regulation (financial integrity) rules. AML rules seek to minimize criminals' and terrorists' ability to use the

185. For example, PSD2 requires the European Banking Authority to develop regulatory technical standards for payment service providers. *See* Directive 2015/2366, *supra* note 18, art. 98.

186. *See* Rodney J. Garratt & Maarten R.C. van Oordt, *Privacy as a Public Good: A Case for Electronic Cash*, 129 J. POL. ECON. 2157, 2157 (2021) (arguing that with the disappearance of cash, digitalized transactions are the intermediaries of digital payments with information that can skew the market).

187. Ellie Rennie & Stacey Steele, *Privacy and Emergency Payments in a Pandemic: How To Think About Privacy and a Central Bank Digital Currency*, 3 L., TECH. & HUMS. 6, 14 (2021) (discussing the variety of methods to approach ensuring privacy in a trend of phasing out of cash and replacing it with digital payment instruments).

188. Garratt & van Oordt, *supra* note 198, at 2157.

189. Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUR. L.J. 140, 153 (2019) (noting that any real level of fair participation in a democratic society requires a level of "non-domination," which is ensured through a protection of privacy).

190. *See generally* Arner et al., *supra* note 9.

191. Tradeoffs require a prioritization of the policy aims of one branch over those of another. *See* Castellano & Tosato, *supra* note 23, at 1047.

financial system. Consequently, they are based on identifying individuals seeking to access the financial system and the origin of individuals' funds. AML regulation seeks to ensure that assets enter the economy licitly, under legal ownership. As such, AML regulation consists of numerous compliance rules for financial service providers and establishes a growing list of predicate crimes and legal instruments that allow financial regulators and law enforcement to detect and prevent money laundering. Access to, accumulation of, and analysis of financial and other forms of data is central to achieving the goals of the AML regime, yet this access is being restricted with increasing frequency by data privacy rules in other jurisdictions.

The international regulatory framework for AML requires intermediaries, particularly financial intermediaries such as banks, and law enforcement agencies to collect data to ensure compliance with AML rules. Under AML regulations, financial institutions are managed through a risk-based assessment (RBA) framework created by the Financial Action Task Force (the main international AML standard-setting body).[192] Per the RBA framework, each financial services provider must create risk profiles for their clients, products, corresponding banks, and other parts of the financial service supply chain.[193] These profiles are made up of data that banks must collect through their own services, affiliates, or other sources.[194] Law enforcement and financial intelligence agencies also use data to develop similar risk profiles.

Issues between dispositive rules and AML have emerged in the context of open finance rules. These issues are most apparent in the European Union. In the European Union's open banking system, retail consumers have control over their financial data. However, financial institutions are responsible for classifying the different types of data that they process, including creditworthiness, customer preferences, and transaction histories. In the European Union, PSD2, which mandates the open banking regime, requires a level of data protection for personal data yet provides an exception for processing personal data by obligated entities when "necessary to safeguard the prevention, investigation and detection of payment fraud."[195] A more recent law, GDPR, establishes a higher level of data protection that, while providing similar exceptions as PSD2, only applies when processing personal data in "criminal cases," not general collection.[196] The European Data Protection Board clarified that the GDPR provides a higher level of protection for personal data while

192. *See generally* FIN. ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH: THE BANKING SECTOR (2014), https://www.fatf-gafi.org/media/fatf/documents/reports/risk-based-approach-banking-sector.pdf.

193. *Id.* at 17–19.

194. *Id.*

195. *See* Directive 2015/2366, *supra* note 18, art. 94.

196. *See* Regulation 2016/679, *supra* note 19, art. 2; *see also Guidelines 06/2020 of the European Data Protection Board on the Interplay of the Second Payment Services Directive and the GDPR*, at 5–6 (Dec. 15, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf [hereinafter *Guidelines 06/2020*] (examining the differences between PSD2 and GDPR).

PSD2 distinguishes protections for data that may comprise personalized security credentials, which may be used for fraud.[197]

The difference between dispositive data governance rules across legal domains has tangible consequences. In 2019, the European Data Protection Supervisor (EDPS) ceased operations of FIU.net—a core tool for the exchange of financial intelligence between member states operated by Europol—due to the site's exchange of information of persons not under criminal investigation.[198] In early 2021, a similar conflict led the EDPS to require Europol to delete huge databases on individuals who were similarly not under criminal investigation and therefore should not have had their data stored.[199] As a consequence of Europol and law enforcement agencies losing access to shared data at Europol, AML supervisors, which are often embedded into such agencies, also lost access to data for operational, tactical, and strategic intelligence gathering.

Thus, there is a clear need for coordinating objectives and content in the context of data governance. This is the case both from the standpoint of industry seeking to comply with the conflicting requirements of data and financial regulation and from a broader policymaking standpoint. A siloed approach, such as the European Union's approach to personal and financial data rules, is no longer possible.[200] Financial data governance must balance competing regulatory objectives.

B. TERRITORIALIZATION AND DATA LOCALIZATION

The second level of challenges to the free movement of global financial dataflows involves jurisdictions' growing tendency toward data territorialization.[201] Data territorialization is the demarcation of digital space.[202] It involves asserting digital sovereignty through rules governing 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 Aadhaar 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 impacted by

197. *Guidelines 06/2020*, *supra* note 196.

198. 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. EUR. CRIM. L. 351, 373 (2020) (discussing how financial intelligence units are particularly prone to data protection issues in the European Union because of their at times administrative entity status).

199. Council Conclusions, *supra* note 25.

200. *See* Emilios Avgouleas & Alexandros Seratakis, *Governing the Digital Finance Value-Chain in the EU: MIFID II, the Digital Package, and the Large Gaps Between!*, *in* DIGITAL FINANCE IN EUROPE: LAW, REGULATION, AND GOVERNANCE 1, 5 (Emilios Avgouleas & Heikki Marjosola eds., 2021).

201. Arner et al., *supra* note 9, at 678.

202. *Id.*

territorialization policies, as are the objectives of financial data governance models such as financial stability, national security, and competitiveness.

In most cases, territorialization policies have been designed to carve out financial data. Financial data needs to be free to traverse jurisdictions so that consumers and financial entities can access international markets, fulfilling the goal of financial stability and helping the economy function. This necessity is exemplified by the special status financial data receives in bilateral trade agreements, such as those enacted by the United States, European Union, and China.

Preferential trade agreements prohibit jurisdictions' ability to limit the movement of financial data. The agreement between the European Union and Japan, for example, prohibits measures preventing the "transfers of information or processing of financial information" necessary to the conduct of ordinary business of a financial service supplier.[203] Stipulations like these expressly set financial services as a priority, setting the tone for the use of financial data for holders, aggregators, and processors. These priorities depend on the interpretation of the ever-evolving characterization of financial services.

A second express priority of jurisdictions' data governance models is to ensure financial stability and market integrity. To this end, free trade agreements have special carveouts that allow financial service providers access to data to regulate domestic financial markets. For example, the agreement between the United States, Mexico, and Canada ("USMCA") recognizes the "immediate, direct, complete, and ongoing access" of regulatory authorities to information that is "critical to financial regulation and supervision."[204] The USMCA further specifies data access for the sake of maintaining market integrity, safety, and financial responsibility.[205]

Following the free-market regulatory style, the USMCA also prohibits requirements on local data storage. However, this prohibition is only applicable if the financial regulator already has "immediate, direct, complete, and ongoing" access to the data it needs to fulfill its regulatory and supervisory mandates.[206] The lack of necessary access to data relevant for financial supervisory goals can trigger disputes. Consequently, the data-access paradigm is a data-localization requirement, because in order to access certain data, the data must be made available in that jurisdiction upon request.

---

203. Agreement Between the European Union and Japan for an Economic Partnership, EU-Japan, art. 8.63, July 17, 2018, 2018 O.J. (L 330) 1, 88, http://publications.europa.eu/resource/cellar/5805924c-09a3-11e9-81b4-01aa75ed71a1.0006.01/DOC_1 [hereinafter EU-Japan EPA]. The USMCA similarly has a provision prohibiting the prevention of data transfer into and out of the territories of the parties. *See* Agreement Between the United States of America, the United Mexican States, and Canada, Can.-Mex.-U.S., art. 17, July 1, 2020, Off. of U.S. Trade Rep., https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between [hereinafter USMCA].

204. USMCA, *supra* note 203.

205. *Id*. art. 17.11(1).

206. *Id.* art. 17.18(1)–(2).

The Free Trade Agreement Between China and Korea ("FTA") sets rules similar to the USMCA. The agreement similarly provides a carveout that allows parties to "adopt measures for prudential reasons."[207] The scope of possible prudential protections is wide, extending to protecting investors and ensuring financial integrity and stability, among other things.[208] However, following China's shared-banking principles, the agreement contains no limitations on data-localization measures specifically, and territorialization more broadly.[209] Depending on its interpretation, the prudential carveouts in the FTA could provide an equivalent level of access to the financial data of third-country subjects as under the USMCA, irrespective of the other data provisions.

Though there are clauses in all three agreements that limit the disclosure requirements for financial data a jurisdiction can enact, they are all relatively minor. All three agreements expressly prohibit financial institutions from disclosing information relating to the affairs and accounts of individual customers, as well as confidential or proprietary information possessed by public entities.[210] However, there is an implied right for financial service providers to transfer personal client information to the servers of other banks across jurisdictions. This is a significant divergence from the hard prohibition on personal data transfer in China, or the extraterritorial personal data protection requirement of the GDPR.

Though free trade agreements highlight the exceptional nature of financial data, such exceptionalism is increasingly eroded by other policy priorities. As the application of broader data governance styles to financial data grows, the free-movement paradigm of financial data is increasingly entering the ambit of other data-related priorities like general data territorialization. This encroachment can take place by embedding financial data into systems controlled by other areas of law, thereby becoming integrated with and inextricable from other rules.

An example of the territorialization of financial data is open finance. By mandating certain technical levels of interoperability from banks through data portability or API standards, client financial data is integrated into a broader, usually domestic data system. For example, the India Stack enables the use of financial services through local Aadhaar digital ID, the standardized unified payment interface, so that data aggregators and fiduciaries can verify data-access rights.[211] Once bound to the India Stack, data cannot move freely between jurisdictions because of a lack of technical interoperability within the Stack as

207. Free Trade Agreement Between the Government of the People's Republic of China and the Government of the Republic of Korea, China-S. Kor., art. 9.5, June 1, 2015, Ministry of Com. China, http://fta.mofcom.gov.cn/korea/annex/xdzw_en.pdf.

208. *Id.*

209. *See generally id.*

210. *Id*. art. 9.4; *see* USMCA, *supra* note 203, art. 17.8; EU-Japan EPA, *supra* note 203, art. 8.65.

211. Carrière-Swallow et al., *supra* note 89, at 13.

well as the variety of personal data, certification, and other rules protecting data within the Stack.[212]

More significantly, the trends of data financial governance follow the ring-fencing trends in the aftermath of the 2008 global financial crisis. After 2008, cross-border finance moved away from the general branch model and toward separately incorporated, capitalized, and regulated subsidiarity requirements in individual jurisdictions.[213] Similar trends toward "ring-fencing" and localization of regulatory, customer, and risk management data of regulated financial institutions have emerged, erecting information walls between data holders and isolating data even within a group of companies.[214] In this context, an increasing range of financial regulators around the world require not only customer data, but also regulatory and risk management data to be held domestically, accessible in onsite servers, or at least available for regulators' immediate and unconditional access.[215] With the digitalization of finance, this trend poses a significant challenge to the dominant operating paradigm of the global digital financial services industry: the free flow of data across jurisdictions that can be controlled, used, and analyzed to meet business objectives, risk management needs, and regulatory requirements.

These data territorialization requirements are driven by jurisdictions' financial stability concerns. These are, for example, the need for regulators to access data to meet their mandates, as well as to safeguard core systems of financial institutions and infrastructure—a major concern over the past twenty years as a result of 9/11 and Y2K. Similarly, there are growing national security concerns, particularly relating to cybersecurity, as well as geopolitics. There are also competition concerns as jurisdictions seek to maximize the benefits of financial data within a certain financial data governance strategy, increasingly in tandem with a wider general data governance approach.

The question that emerges from financial data-localization trends is significant. For the financial industry, data-localization requirements—particularly when a jurisdiction's extraterritorial reach over data conflicts with the localization requirements of another jurisdiction—are an impossible burden, one that will undermine both the benefits of cross-border finance as well as

212. *Id.*

213. After the global financial crisis, one commentator found that more coordination between macroprudential stability tools and monetary policy was required to reduce information asymmetry and increase financial stability. *See generally* Schan Duff, *The New Financial Stability Regulation*, 23 STAN. J.L. BUS. & FIN. 46 (2018). To enable the utilization of these instruments, domestic licensing standards were made more rigid across the world, providing local governments with more information and venues of intervention. *Id.*

214. Ring-fencing is achieved by structurally separating retail banking from investment banking, ensuring that retail activities are performed by a separate entity within the banking group with its own governance regime and restrictions on dealings with the rest of the group, including information sharing. *See generally* Alison Lui, *Retail Ring-Fencing of Banks and Its Implications*, 13 J. BANKING REG. 336 (2012).

215. In 2016, U.S. Treasury Secretary Jack Lew announced a proposal to include financial services within the scope of data provisions in future U.S. trade agreements to ensure the Federal Reserve had access to prudential data, in response to lack of access to such data being held offshores by failing American banks during the 2008 global financial crisis. *Id.*

financial regulation and risk management. Localization requirements are also problematic from the standpoint of the overall objectives of global financial stability, market integrity, and consumer protection.

C. DATA GAPS

The third challenge to the paradigm of global financial flows is data gaps. Data gaps are the decrease in access to the information necessary for governments to ensure financial stability and that development goals are met. Data gaps result from growing data-territorialization measures, which increase the opaqueness of the financial market.

Data gaps present an obstacle to global financial stability, which is underpinned by a complex international system of rules. The development of the nonbinding soft law system has been responsive to the evolving risks to financial stability, bolstering data collection and financial standards. The Basel Committee was established after disturbance in international currency markets in the 1970s and has continued to develop standards for financial services supervision.[216] For example, Basel III responded to the 2008 global financial crisis by creating higher global minimum capital and risk management requirements.[217] Similarly responsive have been international data collection initiatives such as the IMF Standards for Data Dissemination established in 1997 in response to the lack of data preempting the Asian financial crisis, which enable the sharing of domestic economic and financial data for the purpose of increasing global macroeconomic stability.[218] The electronic and statistical data exchanged in this framework of international financial stability creates an iterative feedback loop of learning where the impact of financial policies is understood through collected data. As data sources halt participation in such initiatives because of territorialization in their jurisdictions, data gaps appear.

Many of these gaps stem from the datafication of financial services. As data governance becomes fragmented, so does financial data governance. New data-localization requirements create risks of regulatory arbitrage. For example, while international soft law sets a wide range of standards for financial data standardization and regulatory cooperation, in many cases, these standards lack sufficient granularity. Likewise, despite shared data governance objectives between jurisdictions and the well-developed financial standard-setting architecture, geopolitical, national security, and competition challenges around data are increasing. For example, financial data is increasingly interconnected with personal data, or data of national security concern, and can no longer be

216. *History of the Basel Committee*, BIS, https://www.bis.org/bcbs/history.htm (last visited Jan. 28, 2023).

217. *Id.*

218. Data on government finances—in particular foreign exchange reserves and government debt—were found to be severely lacking. *See generally* IMF, THE SPECIAL DATA DISSEMINATION STANDARD: GUIDE FOR SUBSCRIBERS AND USERS (2007), https://www.elibrary.imf.org/view/book/9781589065550/9781589065550.xml. Note that other well-developed initiatives exist in a range of contexts through other international financial and regulatory cooperation and standard-setting organizations.

easily isolated and exchanged. The result is that even as new sources of financial data emerge via fintech, RegTech, SupTech or other technology-driven digital businesses and tools,[219] their haphazard integration into the existing financial regime may increase market opaqueness and create new blind spots for regulators. These blind spots, in turn, can create novel risks.

New data-driven fintech remains a "wild west" for financial regulators. While the supervisory and reporting expectations for traditional banking activities are clear, especially regarding the requirements for bank balance sheets and risk management, they are not for new digital financial service providers.

This lack of clarity is, in part, due to the unbundling of financial services enabled by digitalization. Virtually the whole bank can be divided into its constituent parts, from origination, intelligence, and risk management to operations, which can then be provided as individual services to businesses, individual customers, or other banks.[220] This can include customer-facing processes like user identification and authentication, chatbots, or claims management. It can also pertain to internal operations like lending, payments, risk scoring, underwriting, or fraud detection.[221] Many of these processes can be provided by non-licensed third parties that have a variety of different disclosure and reporting standards under varying licensing regimes.[222]

The difficulty in regulating fintech extends to the most basic level of regulatory supervision. The surge of new types of fintech products and services, and the rise of nonfinancial enterprises providing these services, is resulting in transnationally divergent approaches to their classification, and thus also to which regulators should supervise them.

The example of how a single fintech entity, in this case PayPal, is beholden to different disclosure and reporting standards across borders demonstrates how it may be difficult to collect financial data when it is unclear who has supervisory authority over a fintech entity.[223] Under the dual banking system of the United States, the legal status of a financial company is partly determined at the state level.[224] Until now, nonbanks were not under the purview of federal banking regulators; nonbanks were subject to state regulatory authorities, licensing and

219. PETER ZETTERLI, CGAP, THE GREAT UNBUNDLING (2021), https://www.cgap.org/sites/default/files/publications/slidedeck/2021_11_SlideDeck_The_Great_Unbundling.pdf (discussing how technology is making financial services modular and how it helps inclusion).

220. *Id.*

221. *Id.*

222. Zachariadis, *supra* note 84, at 132.

223. For example, among the licenses that PayPal has across dozens of states are money lender, sale of checks, installment, escrow law, and financing law licenses—each of which correspond to different state regulation. *See PayPal State Licenses*, PAYPAL, https://www.paypal.com/us/webapps/mpp/licenses (last visited Jan. 28, 2023).

224. PayPal, for example, is regulated in the United States by the CFPB and at the state level as a licensed money transmitter. *See Institutions Subject to CFPB Supervisory Authority*, CONSUMER FIN. PROT. BUREAU, https://www.consumerfinance.gov/compliance/supervision-examinations/institutions/ (last visited Jan. 28, 2023); *About NMLS Consumer Access*, NMLS CONSUMER ACCESS, https://www.nmlsconsumeraccess.org/Home.aspx/About (last visited Jan. 28, 2023).

examination law, and reporting requirements and other consumer protections.[225] PayPal, for example, is not a bank, and is neither insured by the Federal Deposit Insurance Corporation nor subject to a federal prudential regulator.

Similarly, in the European Union, member states can decide whether certain types of institutions can start operating with an initial capital requirement lower than the €5 million traditionally required for banking institutions.[226] In China, PayPal became the first foreign firm with full ownership of a payment business, receiving a payment services license directly from the central bank—the same license issued to WeChat and Alipay.[227] The services offered in all three jurisdictions are identical, and payments cross jurisdictional borders without friction (with the exception of China). The data-collection requirements on the company activity, however, differ significantly among the United States, European Union, and China, as well as the individual U.S. states. In turn, less and less standardized regulatory data is available from new financial data-driven companies.

At the frontier of opaqueness surrounding fintech regulation are cryptocurrencies. Cryptocurrencies are given varied status in each jurisdiction. Depending on their structure, they are considered a substitute for currency in the United States, while the European Union considers them cryptoassets.[228] In 2021, China banned owning cryptocurrency, but the European Union and the United States have only placed due diligence requirements on virtual-asset providers.[229] There is no system for regulating the vast decentralized finance networks that are growing on hundreds of different blockchains. For example, a novel type of secondary financial market is emerging in the domain of nonfungible tokens, where loans taken in a blockchain-based decentralized finance network can be sold as nonfungible tokens.[230] The same dynamic already supports prediction markets, swaps, and longs and shorts.[231] Because of

225. These issuances were challenged by stakeholders in *Vullo v. Office of the Comptroller of Currency*, 378 F. Supp. 3d 271, 296 (S.D.N.Y. 2019), *rev'd sub nom. Lacewell v. Office of the Comptroller of Currency*, 999 F.3d 130 (2d Cir. 2021).

226. Interview with Marius Jurgilas, Bd. Member, Bank of Lith. (Nov. 8, 2020), https://ec.europa.eu/newsroom/fisma/items/684838. Lithuania, for example, has a minimum capital requirement of €1 million for licensing specialized banks. *Id.*

227. Rita Liao, *PayPal's Ambition and Uphill Battle in China*, TECHCRUNCH (Apr. 28, 2021, 3:22 AM), https://social.techcrunch.com/2021/04/28/paypal-china.

228. The Financial Crimes Enforcement Network has outlined that "pursuant to 31 U.S.C. 5312(a)(3)(D), CVC and LTDA are both value that substitute for currency and are therefore 'monetary instruments' under the BSA." Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 86 Fed. Reg. 3897, 3898 n.4 (proposed. Dec. 23, 2020).

229. *Guanyu Jinyibu Fangfan He Chuzhi Xuni Huobi Jiaoyi Chaozuo Fengxian De Tongzhi* (*关于进一步防范和处置虚拟货币交易炒作风险的通知*) [*Notice on Further Preventing and Dealing with the Risk of Speculation in Virtual Currency Transactions*], ZHONGHUA RENMIN GONGHEGUO ZHONGYANG RENMIN ZHENGFU (中华人民共和国中央人民政府) [CENT. PEOPLE'S GOV'T OF CHINA] (Sept. 15, 2021), http://www.gov.cn/zhengce/zhengceku/2021-10/08/content_5641404.htm.

230. *NFTs and the Derivatives Market*, MEDIUM: CDZEXCH. (Sept. 13, 2021), https://medium.com/cdzexchange/nfts-and-the-derivatives-market-8127ada445df.

231. *Id.*

the decentralized nature of blockchain and the different regulatory approaches being taken, following these fast-growing markets is virtually impossible.

These challenges in consolidating significant data gaps, as well as the opportunities for regulatory arbitrage, have systemic implications. The divergence in government approaches to regulating fintech and the difficulty in monitoring their derivative financial data is resulting in a lack of transparency regarding local, and thereby international, fintech markets. This includes a lack of understanding around the types of operations, counterparties, interest rates, terms, and even currencies (including cryptoassets) used in payment operations. Without this information, it is difficult to ascertain the size of relationships between fintech entities and other financial entities, as well as fintech's funding and credit exposures by sector.

V. ADDRESSING THE CHALLENGES OF FINANCIAL DATA GOVERNANCE: MOVING BEYOND THE DATA CENTRALIZATION PARADIGM

Will financial data territorialization, localization, and competition fundamentally upset financial globalization? Or will data gaps and regulatory arbitrage caused by financial data localization sow the seeds of the next financial crisis? We suggest that data localization will remain the status quo of financial data regulation for a variety of reasons. Localization is critical for jurisdictions to fulfill policy objectives. However, localization often results in data collection, processing, or reporting standards that lack interoperability with the financial data of other regimes. The variety of licensing frameworks means that the same entity may be required to generate different data in different jurisdictions.

In contrast to the view of many in the financial services industry, we argue that the existing international financial regulatory architecture, combined with new technologies, can address the most severe risks of conflict and fragmentation.

A. THE INTERNATIONAL FINANCIAL ARCHITECTURE: ADDRESSING NEW CHALLENGES

Unlike transnational data governance,[232] 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, as well as cooperation in cross-border

232. *See generally* Arner et al., *supra* note 9; INST. OF INT'L FIN., STRATEGIC FRAMEWORK FOR DIGITAL ECONOMIC COOPERATION (2021), https://www.iif.com/portals/0/Files/content/Innovation/10_11_2021_digital_economic_cooperation.pdf (arguing for the need of a new permanent structure to help guide international digital economic cooperation); VIKRAM HAKSAR, YAN CARRIÈRE-SWALLOW, ANDREW GIDDINGS, EMRAN ISLAM, KATHLEEN KAO, EMANUEL KOPP & GABRIEL QUIRÓS-ROMERO, TOWARD A GLOBAL APPROACH TO DATA IN THE DIGITAL AGE (2021), https://www.imf.org/-/media/Files/Publications/SDN/2021/English/SDNEA2021005.ashx (presenting a case for global data policy frameworks).

enforcement in market conduct and integrity, with well-developed cross-border cooperation and information sharing in the contexts of payments, banking, and securities.

In the context of finance, well-functioning cooperation mechanisms already exist and can be leveraged to facilitate the circulation of financial data. For example, an answer to financial data circulation may lie in the work from the Committee on Payment and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) on the harmonization of critical data elements (CDE) in OTC derivative transactions and their reporting to trade repositories. In 2018, CPMI and IOSCO issued Technical Guidance for the Harmonization of Critical OTC Derivatives Data Elements, providing guidance on the definition, format, and allowable values of critical data elements.[233] Building on Legal Entity Identifiers, Unique Transaction Identifiers, and Unique Product Identifiers reported to trade repositories and authorities, the final list of harmonizable CDE has 110 items that standardize cornerstone information. This information includes counterparty; beneficiary; and clearing, trading, and settlement data, and allows for more granular approaches to collateral, margins, prices, and other details.[234] These elements aim to remain technologically neutral, allowing a range of technological applications. At the same time, by setting standards for the creation and use of various forms of financial data, they also set the required parameters for technologies used to create, store, protect, use, and transfer data.

More broadly, general initiatives to ensure the exchange of financial data can be taken at the international level. The G20, through the work of the second phase of the Data Gaps Initiative (DGI), expands the focus on data harmonization from just derivatives to broader statistical figures tied to monitoring risks, vulnerabilities, and interconnections in the financial sector. Through initiatives like the IMF Special Data Dissemination Standard Plus,[235] data is increasingly cached on sectoral "deposit-taking corporations" and "other financial corporations," including novel fintechs.[236] Thus, more of the available financial statistical information is used to pursue micro- and macro-prudential data collection through an increasingly harmonized global rulebook that includes the United States, European Union, and China.

As financial data harmonization increases, current due diligence disclosure requirements need to be expanded. Necessarily, this will result in a more

233. *See generally* COMM. ON PAYMENTS & MKT. INFRASTRUCTURES, BD. OF THE INT'L ORG. OF SEC. COMM'NS, TECHNICAL GUIDANCE: HARMONIZATION OF CRITICAL OTC DERIVATIVES DATA ELEMENTS (OTHER THAN UTI AND UPI) (2018), https://www.bis.org/cpmi/publ/d175.pdf.

234. *Id.*

235. This includes findings on net foreign assets and domestic claims on the government, depository corporations, other sectors, shares, and other liabilities.

236. IMF, THE SPECIAL DATA DISSEMINATION STANDARD PLUS: GUIDE FOR ADHERENTS AND USERS (2013), https://www.imf.org/-/media/Websites/IMF/imported-full-text-pdf/external/pubs/ft/sdds/guide/plus/2013/_sddsplus13.ashx.

assertive utilization of RegTech and SupTech solutions capable of drawing on more timely data and combining data from a variety of sources to build prudential models for traditional and novel financial services.[237] These systems will depend on coordinating 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.

Challenges with financial data will remain. Differences between statistical and supervisory reporting standards (like capital reporting templates COREP and financial reporting templates FINREP) can still skew data on account reports, especially when multiple transnational entity linkages are compared. As new business models in the financial sector develop, these differences will have to be ironed out to ensure that fintechs and other novel financial service providers do not cause further regulatory fragmentation.[238] New or existing international fora, like the Global Financial Innovation Network, which counts the United States, many EU member states, and Chinese authorities as participants,[239] would provide a platform for exchanging regulatory practices and vital information.

More profoundly, a stronger institutional framework at the international level might be needed. A key risk is that the fragmentation, in various guises,[240] will fracture the existing international financial architecture. Owing to its iterative collective evolution, the global financial architecture has continued to function more effectively than most other aspects of international cooperation. 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.[241]

---

237. *See generally* GLOB. FIN. INNOV. 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).

238. For an example of federated approaches to financial data sharing, see generally Marina Cernov & Teresa Urbano, *Identification of EU Bank Business Models: A Novel Approach to Classifying Banks in the EU Regulatory Framework* (Eur. Banking Auth., Working Paper No. 2, 2018), https://op.europa.eu/en/publication-detail/-/publication/da027419-4c80-11ea-b8b7-01aa75ed71a1/language-en/format-PDF.

239. *See generally* CHARLES R. TAYLOR, CHRISTOPHER WILSON, EIJA HOLTTINEN & ANASTASIIA MOROZOVA, FINTECH NOTES: INSTITUTIONAL ARRANGEMENTS FOR FINTECH REGULATION AND SUPERVISION (2020).

240. *See generally* Letter from Mark Austen, Chief Exec. Officer, Asia Sec. Indus. & Fin. Mkt. Ass'n, to Randal K. Quarles, Chair of the Fin. Stability Bd., Bd. of Governors of the Fed. Rsrv. Sys. (Apr. 18, 2019), https://www.asifma.org/wp-content/uploads/2019/07/asifma-letter-on-gfma-data-mobility-principles-f20190418.pdf; ASIFMA & OLIVER WYMAN, ADDRESSING MARKET FRAGMENTATION THROUGH THE POLICYMAKING LIFECYCLE (2020), https://www.asifma.org/wp-content/uploads/2020/08/asifma-fragmentation-paper-f20200804.pdf (presenting emerging examples of market fragmentation tied to sustainable finance, data privacy, AML compliance, and operational resilience).

241. *See generally* Arner et al., *supra* note 9; INST. OF INT'L FIN., *supra* note 232; HAKSAR ET AL., *supra* note 232.

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

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

B. TECHNOLOGICAL SOLUTIONS: MOVING FROM FINANCIAL DATA CENTRALIZATION TO DECENTRALIZATION

In addition to the harmonization and reinforced architectural framework supporting financial data governance, the financial sector is uniquely positioned to develop technological solutions to the challenges of data localization and territorialization. Different technological systems have been developed to provide safe solutions to exchanging data.[242] All of these systems have originated from the genesis format.[243] Under this model, the data collector has exclusive control over collected data.[244] However, there are also other models for data collection. For example, "[u]nder the data trust model, legal trusts would be created to hold data, in which fiduciaries manage what the data is used for and who has access to it."[245] Trusts would hold data across jurisdictions and offer a variety of risk appetites and management structures, allowing preauthorized pools of data to be sent to appropriate third parties.[246]

"[J]urisdictions could agree on networks of rules establishing how and what data can be transferred and through which channels."[247] A variety of technologies are already available to help transfer data, from "blockchain applications to security-by-design solutions that can help guarantee security of transmissions medium, to AI that can rapidly analyze the content of transmitted data."[248] For example, the Society for Worldwide Interbank Financial Telecommunications (SWIFT), or other systems of payment messaging and credit card messaging, could adopt such a system.[249] "Data from local banks could be transmitted to a central standardized unit to automatically process" whether and where the data is allowed to route through in accordance with

242. *See generally* Bruno Carballa Smichowski, *Alternative Data Governance Models: Moving Beyond One-Size-Fits-All Solutions*, 54 INTERECON. 222 (2019).

243. *Id.*

244. *Id.*

245. *See generally* Arner et al., *supra* note 9; Sylvie Delacroix & Neil D. Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIV. L. 236 (2019).

246. Other forms of data governance archetypes are closed, single source, data clearinghouse, data pool, and distributed. In a closed system, there is no sharing between data users and data holders. In a single source system, data holders receive data directly from data users. In a data clearinghouse system, there is an intermediary through which data holders can provide data to data users. In a data pool system, data holders pool data to an intermediary, which data users can access. The intermediary also reverts data to original data holders from the data users. In a distributed system, data holders and data users are intermingled. *See* Delacroix & Lawrence, *supra* note 245, at 252.

247. Arner et al., *supra* note 9, at 291.

248. *Id.* at 291–92.

249. *Id.* at 692.

agreement from jurisdictions.[250] This is similar to how Qualified Trust Service Providers under the EU PSD2 regime certify digital ID certificates by pinging back to domestic authorities. These kinds of rules will be vital for critical functions like cybersecurity, market integrity, and increasingly sustainable financing, by setting 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 new technologies are able to offer their products and services without needing to interfere with or even directly access the data of other entities in or across other jurisdictions. Federated data systems use cloud data centers to divide bundles of data across many different systems, ensuring that no party has a data monopoly.[251] These cloud data centers can ensure that data is always accessible through cloud infrastructure.[252] Through federated data analytics, banks and supervisors may not need to access the data of other parties at all; instead, they can run the necessary portion of data analytics locally. Additionally, zero knowledge proof protocols enable secure responses from federated or decentralized data systems without any access to or knowledge of the underlying data.[253] Thus, from the standpoint of finding an international infrastructure for financial data, decentralized structures offer potential approaches.[254]

Change in technology and policy approaches would mean evolving from the dominant paradigm of financial data centralization to one focused on federated storage and analytics. We argue that such a transition would not only be the best way to address the fragmentation challenges of financial data governance, but would also achieve the broader objectives of financial stability, market integrity and efficiency, and consumer protection. More than anyone else, the financial services industry and its regulators are well positioned to make

250. *Id.*

251. *See generally* WORLD ECON. F., FEDERATED DATA SYSTEMS: BALANCING INNOVATION AND TRUST IN THE USE OF SENSITIVE DATA (2019), http://www3.weforum.org/docs/WEF_Federated_Data_Systems_2019.pdf (discussing federated approaches to sensitive data in healthcare).

252. *See generally* FIN. STABILITY BD., THIRD-PARTY DEPENDENCIES IN CLOUD SERVICES: CONSIDERATIONS ON FINANCIAL STABILITY IMPLICATIONS (2019), https://www.fsb.org/wp-content/uploads/P091219-2.pdf; FIN. STABILITY BD., REGULATORY AND SUPERVISORY ISSUES RELATING TO OUTSOURCING AND THIRD-PARTY RELATIONSHIPS: DISCUSSION PAPER (2020), https://www.fsb.org/wp-content/uploads/P091120.pdf (presenting benefits and risks of third-party reliance).

253. *See* Teresa Alameda, *Zero Knowledge Proof: How To Maintain Privacy in a Data-Based World*, BBVA (June 23, 2020), 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 62 (2018) (B.A. thesis, Harvard Coll.), https://dash.harvard.edu/bitstream/handle/1/38811528/GOWRAVARAM-SENIORTHESIS-2018.pdf?sequence=3&isAllowed=y (introducing how zero-knowledge proofs can be used in finance through a variety of examples, mostly tied to disclosing information without showing financial holdings).

254. *See generally* Douglas W. Arner, Dirk A. Zetsche, Ross P. Buckley & Janos N. Barberis, *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, 20 EUR. BUS. ORG. L. REV. 55 (2019).

this transition a necessary part of the ongoing datafication of finance and its regulation.

CONCLUSION

In this Article, we introduce financial data governance. The coalescence of data governance styles, financial regulation, and personal financial data regulation, such as open banking and open finance policies, leads to a variety of financial data governance models. This Article's comparative analysis reveals that four archetypical data governance models are emerging. These models differ depending on the amount of protection given by jurisdictions to the interests of market participants, individuals, and the public. As legal rules and regulatory regimes that were traditionally separate come together, their concomitant application gives rise to a series of new challenges. Two sets of challenges are most significant.

The first set of challenges is substantive in nature. Financial regulation and data governance have some shared objectives, but often their core objectives conflict. This is the case, for instance, in the clash between privacy rights, which lie at the core of many data governance regimes, and transparency needs in the context of financial data regulations, open finance, and the digitalization of financial services more generally. Drawing from and expanding the notion of CLI, this challenge appears to be better addressed through a policy choice that balances competing objectives. As a result, depending on the governance model, different levels of protection can be attributed to the privacy of individuals at the expense of market dynamics, or to the transparency and efficiency of financial transactions while limiting the protection of individual privacy.

The second set of challenges relates to the growing tension between the globalization of finance and fragmentation of dataflows. The territorialization of financial data is taking place because of jurisdictions' growing focus on digital, financial, and economic sovereignty. This can be seen in jurisdictions' limitations on the circulation of personal financial data. It is also evident in the context of customer and transactions data, which is required to be stored locally for prudential reasons, and company data, which is required to be stored locally for national developmental reasons. A second factor is the lack of interoperability between different financial data regimes. This is particularly evident in the context of OTC derivatives, cryptocurrencies, and global financial institutions. Both of these factors reduce the overall exchange of data, creating data gaps, which risk reducing financial stability and other governmental financial goals.

This Article suggests that financial data territorialization is likely to increase. This may in fact be reinforced by the wide use of sanctions operationalized through digital finance as a result of the Russia-Ukraine war. The trend may be further reinforced by the opaqueness of financial flows stemming from new fintech solutions, which need to store data where that data

can be controlled. A multi-layered solution is required to facilitate essential cross-border access to financial data and digitalized services.

At the most fundamental level, harmonization of processes and rules regulating the gathering and transferring of data is required. Harmonization can be achieved by creating international financial data hubs where different types of data can be shared safely without compromising domestic interests or economic or financial needs. A second means of harmonization involves regulators, industry participants, and individual customers using the technologies of digitization and datafication to store data so that it can be accessed for regulatory objectives. New technologies such as cloud technology, jurisdictionally based datacenters, and blockchain technology all allow for data storage enabling decentralized access, analysis, and general governance of data. These technologies can be used by jurisdictions to meet financial regulatory objectives, data regulatory objectives, and national security and developmental concerns. At the same time, these new forms of decentralized and distributed data storage require new forms of analytics, such as federated-learning and zero-knowledge systems, to maximize the value of data for regulatory, business, personal, and developmental purposes.

Through this analysis, we posit that central to policy, regulatory, legal, and technological solutions is that finance, in most respects, is data. Hence, regulation and private law affecting data will have consequences on the financial system, while financial regulation must deal with the digitalization and datafication of finance. Policymakers, regulators, and market participants must reconceptualize financial data and financial data analytics, moving away from the rules and processes grounded on centralized control toward devising solutions that are grounded in decentralized approaches.

* * *