FINANCIAL DATA GOVERNANCE:

THE DATAFICATION OF FINANCE, THE RISE OF OPEN BANKING AND THE END OF THE DATA CENTRALIZATION PARADIGM

DOUGLAS W. ARNER,* GIULIANO G. CASTELLANO,† ĒRIKS K. SELGA‡

Abstract

Finance is one of the most digitalized, globalized, and regulated sectors of the economy. Traditionally technology-intensive, the financial industry has been at the forefront of digital transformation. Starting from the dematerialization of financial assets and culminating in the post-2008 Global Financial Crisis era of FinTech, the integration of finance and a range of new technologies triggered a process of radical digitalization. Data is no longer just the lynchpin of finance; finance is data. Financial transactions are transfers of data, financial infrastructures, such as stock exchanges and payment systems, are data networks; and financial institutions, like banks and other intermediaries, are data processors – gathering, analyzing, and trading the data generated by their customers.

Financial regulation has been forced to adapt to financial digitalization. In parallel, new sets of rules and principles have been developed to assert sovereignty over the digital world. These rules are increasingly enveloping all critical societal functions, from privacy, to national security. Though emerging regulatory regimes pertaining to financial activities and general data governance rules increasingly intersect, their relationship often remains

[*] Kerry Holdings Professor in Law, RGC Senior Fellow in Digital Finance and Sustainable Development, and Associate Director, HKU-Standard Chartered FinTech Academy, University of Hong Kong; Senior Visiting Fellow, University of Melbourne.
[†] Associate Professor in 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.
The authors gratefully acknowledge the financial support of the Hong Kong Theme-based Research Scheme and the Qatar National Research Fund.

unclear. This paper builds a framework of analysis to address the datafication of finance.

First, we define the notion of financial data governance as an 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 emerging key financial data governance components in the European Union, People's Republic of China, India, and the United States. In this context, the relationship between general data governance, financial regulation, and Open Banking reveals different types of linkages defining a set of archetypical financial data governance models.

Second, we examine the challenges affecting financial data governance. As financial information is digitized and financial assets are datafied, finance is inextricably linked to data governance. The coalescence of financial regulation, new regulatory frameworks for digital finance, and general data governance regimes, however, is not always harmonious. Conflicts arising from the intersection of different, and uncoordinated, regimes threaten to frustrate core policy objectives of stability, integrity, and security, as well as the functioning of the global financial system. In order to address this requires a reconceptualization of the financial data centralization paradigm, both by regulators and by the financial industry.

CONTENTS

I. Introduction

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

Data is thus a strategic priority. Like other strategic assets – land, energy, food, water, capital[5] - governments are seeking to assert sovereign control in an emerging era of multipolar geopolitical competition. Through the implementation of new data-specific policies and regulation, general data governance frameworks are

[1] See Viktor Mayer-Schonberger & Kenneth Cukier, Big Data, 78 (2013) (defining digitization as "the process of converting analog information into zeros and ones of binary code so computers can handle it" and noting that "to datify a phenomenon is to put it in a quantified format to it can be tabulated and analyzed").

[2] On the concept of datafication *see also* Ulises A. Mejias & Nick Couldry, *Datafication*, 8 INTERNET POLICY REVIEW (2019) (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 et al., *Regulating Artificial Intelligence in Finance: Putting the Human in the Loop*, 43 SYDNEY LAW JOURNAL (2021)(developing a framework to address the AI "black box" problem).

[4] Especially in in the context of digital communications, interactions, payments, commerce, and finance, see Douglas W. Arner et al., *Digital Finance, COVID-19 and Existential Sustainability Crises: Setting the Agenda for the 2020s*, No. 1 (2021)(describing the role of the Covid crisis in propelling data aggregation and analytics processes).

[5] As framed by *The Economist* in 2017: "[t]he world's most valuable resource is no longer oil, but data." The Economist, *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.(presenting an argument for the growing importance of data and how it impacts data policy). 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 (2013); 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 JOURNAL OF DIGITAL SOCIAL RESEARCH 65 (2020); Francesca Casalini & Javier López González, *Trade and Cross-Border Data Flows* (2019); 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).

emerging, defining a new set of rights and obligations for stakeholders such as data generators and owners. Rather than a sporadic attempt to regulate a new area, each initiative is building a unique data governance style represented by patterns of specific cultural, political, economic, and legal characteristics. Data governance styles are a characterization of the overarching approach a jurisdiction takes towards data, data flows, and infrastructures. Rooted in different "varieties of capitalism,"[6] styles and modes of regulation,[7] the approaches to governing the various elements of data reflect distinct cultural, political, economic, and legal characteristics of any given jurisdiction. As analyzed elsewhere, the general data governance styles of the largest economies – the European Union, United States, People's Republic of China – are colliding, threatening the paradigm of free transnational data flows and fragmenting the global economy.[8]

Finance is also highly dependent on data and its transnational movement. Since the invention of the telegraph in the 19th century, finance has grown into perhaps the most globalized, digitized, and regulated sector of the modern economy.[9] Underlying this digital transformation, the financial sector has undergone a process of dematerialization of financial assets and processes over the past fifty years, transforming financial products and information into digital data.[10] Hence,

[6] See PETER A. HALL & DAVID SOSKICE, VARIETIES OF CAPITALISM (Oxford University Press Aug. 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*, AMERICAN JOURNAL OF INTERNATIONAL LAW 1 (2021/07/27 ed. 2021). (explaining the different capitalist models between the US and China in the context of international trade relationships). *See also* Beyond Varieties of Capitalism: Conflict, Contradictions, and Complementarities in the European Economy (Bob Hancké, Martin Rhodes, and Mark Thatcher, eds, Oxford University Press 2007) (offering an overview of the application of the varieties of capitalism and a critique in the European context).

[7] Cary Coglianese & Robert A. Kagan, *Regulation and Regulatory Processes* (2007) (presenting varieties of capitalism within regulatory processes); Julia Black, *Learning from Regulatory Disasters*, 10 POLICY QUARTERLY (2014) (introducing regulatory governance as a form of managing risks to achieve a publicly stated objective); Giuliano G. Castellano et al., *Reforming European Union Financial Regulation: Thinking through Governance Models*, EUROPEAN BUSINESS LAW REVIEW 409 (2012). (presenting regulatory models in the EU).

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

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

[10] Campbell Jones, *The World of Finance*, 44 DIACRITICS 30 (2016) (presenting a case for how 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 (Bernardo Batiz-Lazo & Leonidas Efthymiou eds., 2016) (arguing that dematerialization has been fundamental for collateralization, innovation, and inflation); *id.*; John O.

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

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 posit that financial data governance models are emerging and are influenced by – and sometimes deviate from – the evolution of general data governance styles. We define financial data governance as an emergent phenomenon comprising rules, processes, and strategies shaping the legal and regulatory framework pertaining to the digitization and the datafication of finance. With reference to China, India, the EU, and the US, the key components of financial data governance can be framed, shedding new light on jurisdictional models. In this context, the relationship between general data governance, financial regulation, and Open Banking reveals significant interactions.

At its core, financial data governance comprises three components: first, financial regulatory regimes applicable to financial data,[11] typically related to enhancing market efficiency, the regulation of market conduct and fairness, pursuit of market integrity, and financial stability and prudential policies;[12] second, financial

McGinnis, *The Sharing Economy as an Equalizing Economy*, 94 NOTRE DAME L. REV. 329 (2018–2019) (presenting dematerialization as a wider phenomenon that acts as a force that equalizes access to services, products, and ideas).

[11] Financial data is the representation of financial information, concepts, and other phenomena in different (analog or digital) forms and mediums so that they are suitable for communication, interpretation, and processing by human beings or automated systems for the purposes of ; see Chaim Zins, *Conceptual Approaches for Defining Data, Information, and Knowledge*, 58 JOURNAL OF THE AMERICAN SOCIETY FOR INFORMATION SCIENCE AND TECHNOLOGY 479 (2007). (exploring the foundations of information science and formulating definitions for data, information, and knowledge). In this paper, we refer to financial data in the digital format.

[12] The full suite of financial regulation is applicable to financial data. For a discussion of developments in financial regulation generally, see Christina Parajon Skinner, *Regulating Nonbanks: A Plan for SIFI Lite*, 105 GEO. L.J. 1379 (2016–2017)(describing the architecture of financial regulation in the US, 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 Institute for Law and Economic Policy 22nd Annual Symposium: Vindicating Virtuous Claims (in Honor of James D. Cox)*, 66 DUKE L.J. 567 (2016–2017)(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 (2017–2018)(describing how risk-focused regulation has altered financial supervision).

regulatory approaches focused specifically on the use of personal financial data and the datafication of finance, such as credit information sharing rules and emerging Open Banking strategies – designed to facilitate third party access to individual customer financial data held by banks with the consent of the customer; and, third, general data governance styles.[13] As an aggregate of these components, digital finance falls simultaneously into the purview of various regulatory regimes.

Financial data governance is thus a dynamic phenomenon; its core components interact as blurred regulatory contours overlap. Open Banking policies are particularly powerful examples of this dynamic. For instance, in the EU, Open Banking stems from both the need to curb the risk of abuses by financial intermediaries and the general principles of the EU attributing control to individuals over their personal data, a divergence from the scope of financial regulation. The result is a mandatory regime requiring banks to ensure consent-based access to customer data by third parties. Moreover, while Open Banking generally dovetails with general data governance frameworks, in some cases, the general regimes for the treatment of data may have to adapt to Open Banking policies. For instance, to keep the EU example, the Second Payments Directive (PSD2) introduced the concept of Open Banking before data portability more generally was introduced in the general data governance framework established by the General Data Protection Regulation (GDPR).[14] Based on these initiatives, the 2020 EU Digital Finance Strategy seeks to expand Open Banking creating an Open Finance framework;[15] whereas the EU's Digital Strategy aims to to expand this to Open Data more generally.[16] In contrast, in the US, there is as yet no general legislative framework

[13] Open banking is a novel phenomenon that manifests in a variety of new digital financial product and service opportunities, see Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327 (2021)(presenting the concept of "data autonomy" as a measure to introduce open banking in the United States); Germain Bahri & Tabitha Lobo, *The Seven Highly Effective Strategies to Survive in the Open Banking World*, 5 JOURNAL OF DIGITAL BANKING 102 (2020)(presenting several models of open banking, from extending traditional banks into digital banks, to providing modular banking services to non-financial entities); Douglas W. Arner et al., *Open Banking, Open Data and Open Finance: Lessons from the European Union*, SSRN Electronic Journal (2021)(presenting four pillars of open finance; facilitation, data protection, reporting requirements, digital identities); OPEN BANKING (Linda Jeng ed., 2022) 1–20 (Linda Jeng ed., 2022)(presenting data as a transformative evolution in the banking industry).

[14] Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 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), art. 4, 2016 O.J. (L 119) 33 (EU)

[15]European Commission, 'Communication 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',COM (2020) 591 final.

[16] Brett Aho & Roberta Duffield, *Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China*, 49 ECONOMY AND SOCIETY 187 (2020).(outlining how the EU has adopted consumer and privacy-protection oriented regulation to counter growing data-surveillance architecture)

for personal data, only for personal data in specific sectors, especially finance.[17] As a result, Open Banking is led by industry rather than legislation and is moving much more slowly as a result.

Second, owing to their composite and heterogeneous nature, financial data governance models engender tensions when misaligned core components interact. As financial information is digitized and financial assets are increasingly digital data, finance is 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 that are capable of mutually frustrating their objectives arise at the intersections of these regimes.

Thus, an emergent set of challenges pertains to the frictions between data governance and financial regulation regimes. The concomitant application of general data regulation and financial regulation may generate incongruous outcomes, whereby the full access to financial information is limited by data governance regimes. Drawing from the notion of Commercial Law Intersection (CLI),[18] finance-specific regulatory policies and priorities, notably concerned with market integrity and financial stability, are emmeshed with new data-focused priorities, aiming at allocating control over data while protecting domestic interests. Conflicts of this sort manifest directly in the market integrity regulation addressing criminal and terrorist use of the financial system – commonly referred to as anti-money laundering (AML). In a similar vein, conflict may emerge with personal data privacy regulation – a right with constitutional-level protection in all subjects of this study.[19] In particular, regulatory conflicts in the EU over privacy subjects, for example, have resulted in agencies such as Europol having to destroy data on criminal activities and/or ask permission of suspects to use their data.[20]

[17] See generally OPEN BANKING (Linda Jeng ed., 2022).

[18] The CLI phenomenon is ubiquitous and has been identified in Giuliano G. Castellano & Andrea Tosato, *Commercial Law Intersections*, 72 HASTINGS L.J. 999 (2020) (offering an analytical framework to examine CLI and devising a normative approach to address the issues emerging from the lack of coordination in CLIs).

[19] Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the US and the EU?*, 8 PENN ST. JL & INT'L AFF. 49 (2020) (presenting the bases of privacy in the EU, China, and US); Raddivari Revathi, *EVOLUTION OF PRIVACY JURISPRUDENCE–A CRITIQUE*, 60 JOURNAL OF THE INDIAN LAW INSTITUTE 189 (2018)(presenting privacy law in India).

[20] In a urged the European Commission and European Data Protection Board to provide clarification on "how to reconcile the AML/CFT framework with the applicable data protection legislations" to ensure data can be shared between obliged entities and competent authorities. This conflict culminated in a recent order from the European Data Protection Board requiring Europol to erase data 4 petabytes of irregularly collected data. See Council of the European Union, *Council Conclusions on Anti-Money Laundering and Countering the Financing of Terrorism* (2020);

A different set of challenges is observed in the international context. Most notably, different regulatory regimes create tensions that threaten the existing paradigm of globalized, uninhibited digital finance. As domestic data governance styles encroach on the ability of financial data to leave jurisdictions, the operational paradigm of free flow of financial data in global finance is challenged. Financial regulation is a highly harmonized system via a complex soft law architecture, including standard-setting bodies and payment flow networks.[21] Domestic data governance styles are, by contrast, highly territorialized leading increasingly to "digital Berlin walls."[22] The free movement of financial data across borders is the foundation for global payment and settlement systems, interbank communication, central banking functions, financial supervision, and international coordination to ensure the stability and the integrity of the global financial system.

Crucially, limited access to data and the absence of mechanisms to share financial information among regulators and market participants undermine the ability to price, assess, and monitor risks, compromising financial stability, as both the 1997 Asian Financial Crisis and the 2008 Global Financial Crisis demonstrated.[23] 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.[24] No single financial authority could grasp the structure of

European Data Protection Supervisor, *EDPS Decision on the Retention by Europol of Datasets Lacking Data Subject Categorisation* (2022).

[21] Lawrence G. Baxter, *Understanding the Global in Global Finance and Regulation*, *in* RECONCEPTUALISING GLOBAL FINANCE AND ITS REGULATION 28 (Ross P. Buckley et al. eds., 2016) (presenting an interconencted soft-law network via the G20, Bank for International Settlements, Basel Committee on Banking Supervision, and Financial Stability Board, and international financial institutions); Ross P. Buckley et al., *Three Major Financial Crises : What Have We Learned?*, *in* REGULATION AND THE GLOBAL FINANCIAL CRISIS (2020)(highlighting that the soft-law bodies regulating transnational finance are notably stronger than prior to the crisis, but myopic in scope).

[22] The idea of a "splinternet" foresees reversing the decentralization of Internet architecture to allow domestic governments to control and divide traffic around the Internet. See generally Mark A. Lemley, *The Splinternet* (2020); Stacie Hoffmann et al., *Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet*, 5 JOURNAL OF CYBER POLICY 239 (2020) (arguing that the splinternet is also a result of diverging technical standards in internet infrastructure, which until now has been generally standardized globally); Georgieva Kristalina, From Fragmentation to Cooperation: Boosting Competition and Shared Prosperity, Keynote Address (Dec. 6, 2021) (2021) (outlining the current trends of technological decoupling and creation of "digital Berlin walls", with negative impacts for the global GDP).

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

[24] ROSS P. BUCKLEY & DOUGLAS W. ARNER, FROM CRISIS TO CRISIS: THE GLOBAL FINANCIAL SYSTEM AND REGULATORY FAILURE (2011); Richard Berner et al., *The Data Reporting Challenge: US Swap Data Reporting and Financial Market Infrastructure* (Nov. 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3541248.

the global OTC derivatives market.[25] More recently, a combination of financial regulatory requirements (respecting overseas listing), data governance requirements (around national security and protection of individual data), and emerging financial data governance requirements (in the context of financial data aggregation) in China emerging from the listing of Didi on the New York Stock Exchange highlight the potential for further fragmentation.[26] The lack of coordination at the transnational level is, thus, generating new blind spots in the transnational framework for financial supervision. The systemic implications of such gaps are not fully discernable, but they are reminiscent of the issues that emerged during the 2008 Global Financial Crisis.[27]

The combination of these different elements results in composite governance frameworks that, while influenced by broader data policies are developing with distinct independence. For instance, financial data is generally an exception to domestic data localization rules to ensure that global financial flows are not blocked. More broadly, financial data governance is epitomized by the evolution of Open Banking in the EU's PSD2 (requiring banks to allow third parties to access their customer data with consent),[28] as well as a variety of regulatory regimes

[25] 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*, 46 IFC BULLETIN CHAPTERS (2017), https://www.bis.org/ifc/publ/ifcb46z.pdf.

[26] 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. *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/ (last visited Feb. 6, 2022).

[27] Several key elements drive the 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 factors in the GFC, see Steven L. Schwarcz & Lucy Chang, *The Custom-to-Failure Cycle Special Symposium Issue: Custom and Law: Essay*, 62 DUKE L.J. 767 (2012–2013)(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, *The Governance Structure of Shadow Banking: Rethinking Assumptions about Limited Liability*, 90 NOTRE DAME L. REV. 1 (2014–2015)(introducing regulatory fragmentation nodes as the sources of complexity that undermine the stability of the financial system); 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).

[28] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment
Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and
Repealing Directive 97/5/EC, 2007 O.J. (L 319) 1

addressing credit information reporting[29] to the recent US Anti-money Laundering Act that established a federal-level legal-entity digital beneficial ownership registry.[30]

Addressing these issues is central to the future of digital data flows in the global financial system. Different strategies, however, are required. Within jurisdictions, the integration between data and financial systems should be seamless as the process of 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, intended as a means to redress ambiguities and conflicts in law.[31]

Transnational fragmentation should be addressed in a different manner. A variety of scenarios are possible for both transnational data flows generally and also for global finance. Unlike transnational data governance,[32] global finance has a well-developed international framework for coordination, standard setting and information sharing. These frameworks – driven in particular by international cooperation and coordination via the Group of 20, Financial Stability Board 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 developing mechanisms – by regulators and

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

[30] The Anti-Money Laundering Act of 2020

[31] The body of scholarship exploring the notion of coherence is vast. *See generally* 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); Susan 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: PROCEEDINGS OF THE CONFERENCE ON LEGAL THEORY AND PHILOSOPHY OF SCIENCE LUND, SWEDEN, DECEMBER 11–14, 1983, 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 (1983).

[32] Transnational fragmentation is increasingly the result of fundamental differences in policy aims and strategic objectives between jurisdictions, requiring new mechanisms to bridge differences. See Arner et al., *supra* note 11.

industry, technological and legal – to address these new realities. The sharing of data by central banks to the Bank for International Settlements is a strong channel that could benefit from updated legal and technical aspects, for example.[33] In addition, emerging technologies – such as decentralized storage,[34] zero knowledge protocols,[35] and federated analytics[36] – can facilitate industry and regulators both to "store" and use data without requiring to transfer them across jurisdictional borders, a change from the dominant paradigm of centralization of financial data (epitomized by Equifax) to a new paradigm of data decentralization, based on new technologies and new policy approaches.

This paper is structured in six parts: Following this introduction, in Section Two, we discuss the digitization of finance and the challenges which it poses from the standpoint of traditional financial regulatory objectives: financial stability, consumer protection and fairness, efficiency, and market integrity, highlighting the need for recognition of the evolving nature of finance and the legal and regulatory treatment in particular of data in all its forms. In Section Three, we consider the datafication of finance and the intersection of data, finance and data governance, highlighting both emerging general data governance styles as well as the evolution of a range of Open Banking strategies, focusing on personal financial data. In Section Four, we present four emerging financial data governance strategies, exemplified by the US, EU, China, and India, seeking to bring together finance and its regulation with their evolving domestic data governance regimes. In Section Five, we elaborate how the result of differences in these strategies combined with prudential objectives are converging towards territorialization via data localization. We then address this growing challenge of fragmentation in Section Six by outlining how the well-developed transnational regulatory frameworks in finance offer an opportunity to develop technological solutions and approaches which may in fact support both the objectives of financial and data regulation.

[33] Bank for International Settlements, *Data-Sharing: Issues and Good Practices*, No. 1 (2015).

[34] 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 Ethereum, *Decentralized Storage*, ETHEREUM.ORG, https://ethereum.org (last visited Feb. 11, 2022).

[35] Zero knowledge protocols are a form of authenticating an entity or certain data without using the information itself to verify its veracity, allowing communicating information without revealing it to parties that communicate it via mathematical models. *See* Lily Hay Newman, *What Are Zero-Knowledge Proofs?*, WIRED, https://www.wired.com/story/zero-knowledge-proofs/.

[36] Federated analytics allow 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, *Federated Analytics: Collaborative Data Science without Data Collection*, GOOGLE AI BLOG, http://ai.googleblog.com/2020/05/federated-analytics-collaborative-data.html.

II. The Digitalization of Finance

Finance is inextricably linked to the acquisition, analysis and processing of massive volumes of diverse forms of information, today mostly in digital form. Capital markets have been conceptualized as networks of social relationships,[14] where participants send signals about the quality and quantity of different financial products, thus determining their prices.[15] More broadly, financial information, intended as data concerning transactions of businesses and individuals, is the core fuel of modern financial systems. Financial information underlies both the Efficient Capital Markets hypothesis as well as financial regulatory requirements for information disclosure, access, and quality. In addition to investors in stock markets who rely on analysis of information to take investment and trading decisions, lenders, for instance, estimate the credit worthiness of potential borrowers through a variety of financial information, such as repayment history, credit card transactions, income statements, and asset information. A wide range of proprietary but also shared sources such as credit rating agencies, credit bureaus and increasingly a range of Big Data and alternative data sources compound such sources of data, exemplified in the rise of FinTech and BigTech credit.

This Section focuses on the role of digital data in modern finance. First, it illustrates how the evolution of finance, technology, and related legal rules has increasingly focused on data. Such an analysis, in turn, allows to indicate that data is not just a means to encapsulate financial information, but the foundation of modern finance.

A. Finance, Technology, and Law

Finance, technology, and law are co-developmental, paralleling and interacting with the evolution of past and modern civilization.[37] While finance does not entail the production of physical goods, throughout much of human history it has been supported by the physical tools used for accounting purposes, such as documents, books, coins or even stone tablets. In fact, central to any financial activity is the ability to record transactions and the information related to the parties involved; even the simplest money lender's pawn transaction would result in a chit as a record for the borrower and a record in the lender's ledger.[38] 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, paper money (in addition to coins).[39] With

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

[38] *Id.*

[39] *Id.*

electrification, the diffusion of electronic storage and computing power, finance evolved into a digital industry, where financial instruments (such as stocks and other securities) are dematerialized, and financial information is digital.

Ideally, the symbiotic relationship between finance and technology is ultimately aimed at supporting the "real economy,"[40] the portion of the economy concerned with the production of goods and the provisioning of services. Hence, finance, supported by technology, has developed to allocate and deploy economic resources across industries, market participants, and over time.[41] As a result, the financial system has a deep and wide reach, catering to the financing needs of businesses, trade, governments, and individuals. Finance and technology are co-developmental. Starting with the advent of the telegraph in the 19th century, followed by a deeper integration of information technology in finance of the 20th century, leading to the FinTech movement ushered by the 21st century, the local, domestic, and global dimensions of finance have been inextricably intertwined with technological advancements.[42] Today, the global financial system is several times the size of the real economy, and almost entirely digital and dematerialized, exemplified by global foreign exchange market turnover of over US$ 6.5 trillion each day.[43]

Nonetheless, the competitive forces underlying financial markets do not always yield the desired effects. These malfunctions are commonly referred to as "market failures" and represent one of the primary justifications for public (regulatory) interventions in the financial system.[44] Through this lens, financial regulation

[40] 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" in the *Cambridge English Dictionary & Thesaurus*, CAMBRIDGE DICTIONARIES ONLINE, https://dictionary.cambridge.org/dictionary/english/real-economy.

[41] 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 socio-economic function of allocating economic resources across border and time is realized through a sub-set of functions, including the clearing and settling of payments, the management of risks, and the deployment of capital).

[42] Arner et al., *supra* note 12.

[43] The notional volume of derivatives in 2018 was over US$ 500 trillion – approximately eight times the value of global GDP, *See* Servaas Storm, *Financialization and Economic Development: A Debate on the Social Efficiency of Modern Finance*, 49 DEVELOPMENT AND CHANGE 302 (2018); Zoltan Pozsar, *Institutional Cash Pools and the Triffin Dilemma of the US Banking System* (2011).

[44] Although other reasons, such as social solidarity, lend strong support to the implementation of regulatory policies, the market failures rationale – deploying the analytical tools of economics – is commonly considered as the main reasons justifying the regulation of financial markets; see JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION 51 (2016) (noting that the key features of financial markets make them prone to market failures); and Steven L. Schwarcz, *Controlling Financial Chaos: The Power and Limits of Law*, WIS. L. REV. 815, 818 (2012) (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.").

provides a set of rules and principles that instill confidence in the financial system by addressing market failures. The combination of digitalization and financialization highlights an increasing disconnect between finance and the real economy.

More profoundly, and beyond the traditional market failure rationale, sophisticated socio-legal inquiries have indicated that legal and regulatory regimes have evolved with financial markets,[45] leading to consider finance as a legally constructed phenomenon.[46] The social relationships composing financial markets are embedded in and represented by contractual arrangements, conveying critical financial information. Commercial and financial law 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.[47]

In this context, the law evolves and interacts with the technology underpinning finance. As financial assets, such as securities, are dematerialized and, thus, exist and are held electronically in depository systems, legal rules have had to adapt. The legal status, the evidentiary nature, and the enforceability of electronic transactions must correspond to the needs of market participants and function at least as well as those attributed to paper-based transactions. While most of the legal issues concerned with the emergence of electronic financial activities have been debated, and to a large extent addressed, since the second half of the 20th century,[48] new challenges have emerged as the processes of dematerialization ushered a more

[45] Especially important in 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* Simon Deakin, *The Evolution of Theory and Method in Law and Finance*, THE OXFORD HANDBOOK OF FINANCIAL REGULATION. OUP, OXFORD 13 (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 JOURNAL OF COMPARATIVE ECONOMICS 338 (2013) (introducing the legal theory of finance as multi-discipline area of study)

[46] Katharina Pistor, *A Legal Theory of Finance*, 41 JOURNAL OF COMPARATIVE ECONOMICS 315 (2013).(arguing that financial markets are legally constructed and thus law can cause financial markets to collapse); Julia Black, *Learning from Regulatory Disasters*, 10 POLICY QUARTERLY (2014) (introducing regulatory governance as a form of managing risks to achieve a publicly stated objective)

[47] *Id.*

[48] For an early discussion of the challenges posed by the dematerializations of financial transactions and assets, *see* Chris Reed, *The Law of Unintended Consequences-Embedded Business Models in IT Regulation*, JOURNAL OF INFORMATION, LAW & TECHNOLOGY (2007)(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).

profound, and ongoing, transformation. These have been clearest over the past decade with the emergence of new technologies in finance, in particular new forms of digital assets.

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 shifted the focus from the digitization of back-end processes and activities (within financial institutions) to the deployment of digital technologies to delivery financial services to consumers.[49] Second and related, the combination of novel technologies and financial activities of the FinTech movement has promoted the creation of new business models and products, significantly changing existing practices.[50] Third, the diffusion of digital finance and the advancement of FinTech solutions have been supported by the increasing integration of novel technologies.[51] 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 (IoT) are transforming finance.[52]

The digitalization of finance also resulted in the definition of new financial inclusion policies.[53] Digital financial services, ranging from mobile payments to larger platform-based ecosystems using consumer generated data to tailor financial products, are a powerful agent of change pushing industry innovation as well as financial inclusion policies.[54] In fact, digital solutions are instrumental to broaden access to financial services and cater the financing needs of individuals and small business.[55]

To unlock the potential of digital finance, regulatory policies have been focusing increasingly on facilitating the circulation of data, within and across financial industries. In addition to traditional focuses on standardization and regulatory sharing, a notable new example is offered by Open Banking initiatives, whereby

[49] Arner et al., *supra* note 7.
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] Douglas W. Arner et al., *Sustainability, FinTech and Financial Inclusion*, 21 EUROPEAN BUSINESS ORGANIZATION LAW REVIEW 7 (2020)(highlighting how digital finance has been used to address both micro- and macro-economic challenges related to sustainability); MAJID BAZARBASH, FINTECH IN FINANCIAL INCLUSION: MACHINE LEARNING APPLICATIONS IN ASSESSING CREDIT RISK (2019) (discussing how novel technological capabilities like machine learning to help encourage financial inclusion).
[54] Arner et al., *supra* note 7.
[55] *Id.*

payment and banking service providers should ensure that authorized third parties can have access to customer and payment accounts information.[56] While complying with this core objective, however, financial institutions and jurisdictions can adopt a variety of approaches, selecting the level of openness, the type of services, and how to integrate their offerings with the business model of other players.[57] The result is a financial system where financial data becomes a resource to expand the reach of financial services and a commodity that be integrated to new financial services.

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 for the assessment of various risks – based on models calculating the probability of repayment – and for the pricing of different services. It also refers to data about financial markets and products, such as stock prices and accounting data about firms and governments. In a similar vein, the data gathered by financial institutions is routinely used for regulatory purposes: financial institutions are required to gather data to detect suspicious activities in fight against money laundering and financing of terrorism, and market, client, statistical, and transaction data are used determine the level of protection against various prudential risks, including credit risk, market risk, and operational risk.[58]

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

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

[56] See Section III.D. for a more in-depth discussion of Open Banking.

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

[58] For discussions exemplifying regulatory reporting requirements for financial data, *see* Abdullahi Usman Bello & Jackie Harvey, *From a Risk-Based to an Uncertainty-Based Approach to Anti-Money Laundering Compliance*, 30 SECUR J 24 (2017); Patrik Alamaki & Daniel Broby, *The Effectiveness of Regulatory Reporting by Banking Institutions* (2019).

best exemplified in the emergence of Open Banking – an initiative that involves all three core actors.

C. The Datafication of Finance: Finance as Data

The coalescence of finance and data has changed the core nature of financial activities.[59] While critical transformations stem from the financial system, the relationship between finance and data is shaped also by forces resting outside the traditional boundaries of the financial industry.[60] Large non-financial, data-intensive firms (BigTechs), for example, are quickly acquiring the capacity to offer advanced financial services, competing with traditional finance providers, such as banks and investment companies on the basis of their embedded digital networks.[61] These dynamics do not mark a transitory phase, but rather an evolutionary step towards the integration of data and financial systems.[62]

Furthermore, the novel uses of growing amounts of accessible financial and other data together with new technology are extending the frontiers of financial services. For instance, the availability and amount of data is fueling a diffused deployment of AI for retail, professional trading, and compliance purposes. Moreover, the possibility of ensuring the integrity of data in a decentralized fashion, through DLT is prompting profound transformations in the context of supply-chain financing as well as for the development of new classes of assets.[63] In a similar vein, the emergence of cryptocurrencies, digital assets and decentralized-finance (DeFi) is also fueling the decentralization of data and data-related services, with the promise of creating a new financial infrastructure.[64]

In this environment, data is not just a vehicle of financial information; it is a constitutive component of finance. Finance largely is data. The datafication process spurs the acquisition and analysis of new digital data that, in turn, enables the

[59] For an overview of how the finance is being changed by digitalization, *see* Dirk A. Zetsche et al., *Digital Finance Platforms: Toward a New Regulatory Paradigm*, 23 UNIVERSITY OF PENNSYLVANIA JOURNAL OF BUSINESS LAW 273 (2020)(in regard to platformization of finance); Arner et al., *supra* note 9; Helen Bollaert et al., *Fintech and Access to Finance*, 68 JOURNAL OF CORPORATE FINANCE 101941 (2021)(in regards to lending, crowdfunding, and initial coin offerings).

[60] Zetsche et al., *supra* note 62; Arner et al., *supra* note 12; Bollaert et al., *supra* note 62.

[61] Lianrui Jia & Dwayne Winseck, *The Political Economy of Chinese Internet Companies: Financialization, Concentration, and Capitalization*, 80 INTERNATIONAL COMMUNICATION GAZETTE 30 (2018) (describing financialization as the discussing the growth of and financialization of BAT in China).

[62] Arner et al., *supra* note 12..

[63] *Id.*

[64] Linn Anker-Sørensen & Dirk Andreas Zetzsche, *From Centralized to Decentralized Finance: The Issue of "Fake-DeFi,"* SSRN ELECTRONIC JOURNAL (2021).(describing DeFi and highlighting the trend of false decentralization).

development of new technological solutions. The datafication of finance promotes the ever-growing financialization of the modern economy, as financial transactions connect market participants around the world and data are traded within and outside the financial system.[65] Financial instruments, payment systems, trading venues, and compliance functions are part of an ecosystem where data is a representation of information about markets 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 non-physical manner via a digital infrastructure that has a global reach.[66]

III. Financial Data Governance: Regulating the Digitization and the Datafication of Finance

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

This Section considers the evolution of the key components of financial data governance. First, the financial regulatory regimes affecting the digitization of financial information are examined. Thereafter, general data governance styles are introduced. Finally, the section considers the development of Open Banking and its various aspects in different jurisdictions.

[65] Storm, *supra* note 46.(arguing that the "financialization of everything" has facilitated rent-seeking practices).
[66] *Id.*

A. Regulating Financial Data

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

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

In respect to prudential policies, strong attention has been given to the risks emerging from the growing integration of digital systems in financial activities. Technological failures, cyber-attacks, legal actions and regulatory sanctions related to the mistreatment of data are form of operational risk that may compromise the solvency of financial institutions. As data and technology are inextricably related to finance, new international standards have been elaborated to ensure that technology related operational risks are properly addressed. In particular, the Basel Committee on Banking Supervision (BCBS) has launched an epochal overhaul of the rules that banks must implement vis-à-vis the assessment and management of data and technology risk: TechRisk. The result is an increased level of capital requirements to ensure enough loss absorbing capacity against operational risk and the implementation of a principle-based approach to strengthen operational resilience within banks. [67]

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

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

In the context of market integrity, in particular, AML requirements mandate financial service providers to integrate many categories of data into their risk calculations in transactions of different products, clients, or geographies.[68] Under these frameworks, data generally considered protected personal data, like transaction or account data, instead becomes a customer due diligence requirement for the purpose of managing operational risk. This customer-based risk data then plays a variety of functions, being tied also, for example, to suspicious transaction reporting to financial intelligence units or other supervisors.

From a market failure standpoint, a central focus of regulation is on quality and availability of information. Disclosure requirements and information quality assurance regulations of gatekeepers such as accountants, auditors, intermediaries, credit rating agencies and credit bureaus constitute a very large portion of financial regulation and are central to market functioning, investor protection and market participant decision making.

Lastly, financial data is becoming the direct corollary of broader regulatory reporting requirements and supervisory action. Regulators are requiring banking data to be machine-readable to enable supervisory automation processes and more granular data aggregation capabilities.[69] 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.[70] Supervisory technology (SupTech) models are requiring financial data to be structured so that regulators have direct access via automatically packaged business data (data-input approach), through collecting business data directly from bank systems (data-pull approach), through analyzing operational bank data at will (real-time access), or other formats. These SupTech instruments are not only

[68] Banks are expected to consider a range of factors in the RBA, including the nature of their business, target markets, customer risk, jurisdictions the bank is exposed to, distribution channels, etc. *See* FATF, *Guidance for a Risk-Based Approach - The Banking Sector* (2014).(introducing the scope of RBA for financial services and supervisors).

[69] Financial Stability Board, *The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions* (2020).(discussing the drivers, benefits, and challenges of SupTech and RegTech).

[70] Toronto Center, *FinTech, RegTech and SupTech: What They Mean for Financial Supervision* (2017).(presenting the range of utility of RegTech and SupTech, including the novel data analytics uses they open).

expanding the micro-prudential supervisory capacity, but enabling the aggregation of vast data pools for machine-learning and AI solutions used for risk management.

Second, as data is treated as a strategic resource and governance expands its reach domestically and internationally,[71] regulatory regimes concerned with the treatment of financial information naturally intersect and interact with general data policies. In fact, financial data encompasses myriad classes and types of data that, while used for financial purposes, may also fall squarely into the general category (or categories) of data, particularly personal data. The holders and processors of financial data are thus being increasingly directly or indirectly regulated by general data governance rules in force in any given jurisdiction. These general regimes typically establish different rights concerned with the alienability, circulation, or management of personal financial data.[72] However, at the same time financial data – both personal and non-personal – are also the object of specific regulatory initiatives, stemming from sector-specific needs and concerns.

B. The Evolution of General Data Governance Styles

In the past thirty years, economic globalization has been supported by a common approach to data. Originating from a US-led conception, the digital world developed as a permission-less, open, and liberal space, as evidenced by the Internet. Here, individuals, corporate entities, state-actors, and international organizations converged in a global network of networks.[73] Upon these premises, market-like mechanisms gathered and exchanged data that, in turn, became the primary commodity in the digital space. As the links between digital and physical worlds multiplied, owing to the development of new technologies and to the expansion of infrastructural capabilities, a data economy developed and expanded beyond the digital perimeter. From daily tasks personal and professional capacities

[71] Especially, and increasingly in regard to critical infrastructure, and critical functions like national security, financial markets, or transportation. *See* Arner et al., *supra* note 11.

[72] *See Infra* Section V for a discussion of regulatory fragmentation and data territorialization as a result of the emergence of data governance styles.

[73] The Internet has been described a burgeoning "Network of Networks" that enables interaction between many different domains. *See* Sara Helen Wilford et al., *The Digital Network of Networks: Regulatory Risk and Policy Challenges of Vaccine Passports*, 12 EUROPEAN JOURNAL OF RISK REGULATION 393 (2021)(Uses digital vaccine passports as an example of failure and challenges in network of networks); William H. Dutton, *Multistakeholder Internet Governance?* (2015)(argues that the Internet is creating new institutions capable of interacting with entities like governments or industry); Donatella Della Porta & Lorenzo Mosca, *Global-Net for Global Movements? A Network of Networks for a Movement of Movements*, 25 JOURNAL OF PUBLIC POLICY 165 (2005)(Discussing how the Internet empowers social movements instrumentally, cognitively, and symbolically); Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, GLOBAL COMMISSION ON INTERNET GOVERNANCE (2014) (arguing for a need to shift analytical focus from narrow Internet governance regime, to a broader cyber regime complex with a variety of issue-specific actors).

of individuals to critical societal functions, such as payment and healthcare systems, societal dependence on data has become ubiquitous.

As data becomes a strategic asset, nation-states have begun to assert sovereignty over the digital world, both domestically and internationally. Legal and regulatory frameworks are being developed to define rights and obligations for data generators and holders.[74] Competition policies have been triggered to curb data abuse by dominant incumbent firms.[75] New rules to assert control over internal and external data flows and related infrastructure are being enacted.[76] At the heart of these initiatives lies the urge for state actors to assert their sovereignty over data.[77] The result is the emergence of an increasingly fragmented global data governance framework.

Taken together, the domestic efforts to reign the digital world define specific patterns. As argued elsewhere, such patterns create specific data governance styles.[78] Each style is characterized by three sets of variables.[79] The first set describes the overall attitude towards the market for data, stemming from general cultural and political values, as reflected in the variety of capitalism and governance

[74] Rights and obligations for data stakeholders extends across many policy domains. *See generally* Rene Abraham, Johannes Schneider & Jan vom Brocke, *Data governance: A conceptual framework, structured review, and research agenda*, 49 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT 424–438 (2019) (highlighting the evolving state of data governance across domains, within data science, and in organizational scopes); LARRY CATÁ BACKER, *And an Algorithm to Entangle them All? Social Credit, Data Driven Governance, and Legal Entanglement in Post-Law Legal Orders* (2020), https://papers.ssrn.com/abstract=3512608 (last visited Jan 3, 2021) (arguing that the emergence of data driven analytics and algorithmic techniques is reshaping the conception of data governance).

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

[76] These interventions cover a variety of areas of law, and are related to asserting control for the purposes of privacy, competition, socioeconomic development, and other reasons. For more, *see* Arner et al., *supra* note 11..

[77] OECD, THE PATH TO BECOMING A DATA-DRIVEN PUBLIC SECTOR (2019); Un Secretary-General, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere with Insight, Impact and Integrity, 2020-22* (2020). (recognizing the rise of data as a strategic asset around the world and presenting a framework for jurisdictions to mobilize and secure data capabilities).

[78] The locution has been first coined in Douglas W. Arner et al., *The Transnational Data Governance Problem*, forthcoming in BERKELEY TECHNOL. LAW. J. (2022). (presenting a framework for analyzing data governance styles and discussing the emergence of market-based, rights-based, and state-based styles in the US, EU, and China, respectively).

[79] *Id.*

model adopted in any given jurisdiction.[80] The second set of variables describes the core principles guiding policy interventions, thus defining the relationship between individuals and data and the right attributed to data generators and data owners.[81] The third set of variables identify the primary feature of the regulatory and enforcement approach affecting a jurisdiction's data and data flows.[82] Taken together these sets of variables define the data governance style of any given jurisdiction.

Crucially, data governance styles manifest in the cardinal direction taken to regulate data, data flows, and digital infrastructures within and outside domestic borders. When applied to the three major world economies and primary standard-setters – notably, China, the EU, and the US – the domestic trajectories for data governance emerge starkly. Starting from the US, it is clear that a market-based style and a laissez-faire regulatory approach to data and technology have nurtured the rise of the Internet and its current paradigm: globalized, permission-less, and supportive of free trade.[83]

Largely in response to the dominance of American players in the global digital economy, the EU, first, and China, more recently, have developed their own digital strategies. In the EU, the governance style is right-based at it establishes protections for the gathering, the use, and the circulation of personal data of EU citizens, while spurring the emergence of a digital economy within the European Single Market.[84] A more centralized governance style is emerging in China, where a state-based approach treat data and data flow as part of broader policies, ranging from national security and infrastructural autonomy to general socio-economic goals of improving the quality of life of Chinese citizens.[85] The analysis of data governance styles can be extended to other jurisdictions. For example, India is a jurisdiction where data governance focuses on a rights-based approach, while also embracing

[80] This dynamic is assessed through the prism of the political economy framework of "varieties of capitalism," where data governance measures are layered into strategic interactions of key institutional relationships. *See Id.*

[81] Alignment is characterized by the dialogic focus of a jurisdiction, which can be market, individual, or state based. Each alignment propels the apportioning of rights and responsibilities that reinforce the primacy of their principles. *See Id.*

[82] Regulatory mechanisms extend across a continuum between bottom-up, decentered and focused on private actors, or top-down, centered and focused on the public sector. *See Id.*

[83] *Id.*

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

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

utilizing data policy as the main vehicle for the delivery of public goods and services.

Each data governance style connects and interacts with the strategies to regulate financial data and digital finance in various manners. In particular, as financial data encompasses a variety of different classes of general data, from personal to non-personal information, the emergence of data governance styles necessarily intersects with rules and principles designed to regulate financial data and its related ecosystem.[86] More broadly, as data is the object of financial transactions,[87] data governance styles represent a major influence as the financial data governance strategies are developed. Depending on whether a given data governance style promotes or inhibits the digitization and datafication of finance, financial data governance will result in complementarities or exceptionalisms. This connection is particularly evident in the context of Open Banking initiatives, as they presuppose the circulation of data within a given jurisdiction.

C. Regulating the Datafication of Finance and the Emergence of Open Banking

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

For instance, unlike the EU which has had a formal legal framework for personal data since 1995,[88] the US has not had a general legislative framework governing personal data but rather a complex series of federal and state legislation and case law. California adopted the first comprehensive state data protection legislation in 2018, the California Consumer Privacy Act (CCPA), which entered into force in 2020.[89] However, the US has developed legislation in a number of specific areas, including finance. The most significant are the Fair Credit Reporting Act enacted in 1970[90] and amended by the Fair and Accurate Credit Transactions Act of 2003[91]

[86] See supra Section II.A for a discussion of digital data.

[87] See supra Section II.C for a discussion of data as finance.

[88] European Data Protection Supervisor, *The History of the General Data Protection Regulation*, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (last visited Feb. 9, 2022).(describing the development of data protection in the EU)

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

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

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

and the Gramm-Leach-Bliley Act[92] and its creation of the Consumer Financial Protection Bureau (CFPB)[93] specifically addressing consumer financial data. Absent a general data protection framework, these can be seen as sector specific elements of the US general data governance style, albeit ones provide for a sectorally specific set of rules and that may in fact eventually form the basis of a broader set of rules governing personal data in the US.

In contrast, while the EU has long had a general framework for personal data protection, prior to 2018, this had a limited impact in the context of financial data, personal or otherwise. This however changed with the implementation of both PSD2 and GDPR in 2018.[94] PSD2 (adopted in 2015) provides a framework for Open Banking while GDPR (adopted in 2016) provides a comprehensive framework for personal data protection. Together they are central to both the EU's general data governance style and also its financial data governance strategy.

Open Banking parallels and interacts with the general data governance style but also is emerging as a separate yet related strategy, with the EU as first mover and the leading proponent of a mandatory legislative approach, reflecting and extending its more general data governance style. In the EU, PSD2 (which predates GDPR) establishes a framework that promotes the emergence of novel payment-service providers, through a licensing structure that requires banks to provide access to a client's payment account to third parties on the basis of their consent.[95] Banks have to comply with a system of rules that facilitate the transferability of data, by

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

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

[94] Dirk A. Zetzsche et al., *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II*, SSRN Electronic Journal (2019)

[95] MICHAEL R. KING & RICHARD W. NESBITT, THE TECHNOLOGICAL REVOLUTION IN FINANCIAL SERVICES: HOW BANKS, FINTECHS, AND CUSTOMERS WIN TOGETHER 143 (2020) (PSD2 creates a tri-partite system. 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 a payment initiation service provider (PISPs), that offers an online service to initiate a payment order as requested by the user.).

developing APIs that meet a minimum set of functional standards.[96] PSD2 however only mandates sharing by banks, an aspect for which is has been criticized.[97]

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

At the most basic level, Open Banking enables consumer generated data to be transferred (data portability) or accessed by third parties. Approaches can range from legislatively mandated (as in the EU) to industry-led voluntary systems (as in the US), with a range of roles for regulators in between.[98] In mandatory systems like the EU, Australia and UK, core granular provisions have been adopted, mandating financial institutions to grant third-party access to their data, regulating access through APIs, and establishing standardization of digital ID for users. The comparison with different rules offers a useful illustration of how policymakers in different jurisdictions understand and promote Open Banking: Open Banking in one jurisdiction can be very different from Open Banking in another, particularly in the context of its level of legal basis and its interaction with general data governance styles.

Data portability lies at the heart of Open Banking strategies; key variances lie in the degree of portability required. For instance while US federal law does not require information portability (and thus is the basis of a voluntary Open Banking strategy in the US and one which so far has largely been ineffectual as a result of industry recalcitrance despite outward enthusiasm), the California Consumer Protection Act grants users a right to receive their personal information in a useable readable format for easy transmission from their data holder.[99] The EU GDPR provides a similar right, highlighting that the copy of a user's data should be in a commonly used and machine-readable format. Both regimes establish a

[96] Crucially, banks must (1) allow account information service providers (AISPs) and payment initiation service providers (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; (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 EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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), OJ 2016 L119/1.

[97] Douglas W. Arner et al., *Open Banking, Open Data and Open Finance: Lessons from the European Union*, Forthcoming in Linda Jeng (ed), Open Banking (2021)

[98] See generally OPEN BANKING, *supra* note 16.

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

requirement for data holders to initially classify and compartmentalize personal data and to be able to divide it from the rest of their data.

The approach adopted to Open Banking in any given jurisdiction is an important proxy to gauge the trajectory being adopted for financial data governance. In general terms, Open Banking policies are typically concerned with regulating the relationships with: (i) financial data holders, such as banks and other financial institutions; (ii) processors, such as technology-focused and FinTech firms; and (iii) users mostly represented by individuals and small business.[100]

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

Along with the EU, the UK and Australia[101] are typically seen as strongest example of legislatively mandated Open Banking strategies while the US is usually seen as a (so far largely ineffectual) example of an industry led voluntary Open Banking strategy. The EU in fact is moving beyond Open Banking towards Open Finance and eventually Open Data, reflecting the parallel evolution of its general data governance style. In between these extremes lie a range of models, usually characterized by the level of regulatory guidance and involvement, with Singapore and Hong Kong both being characterized by active regulatory encouragement and standard-setting but absent legislative mandates. Singapore in particular has been very active in building infrastructure and implementing regulatory encouragement as the basis of its Open Banking strategy, suggesting the regulator-led approach as a third major form.

China is also developing its own variant of Open Banking. In China, much of the consumer-authorized financial data access takes place through private platforms.

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

[101] Ross P. Buckley et al., *Australia's Data-Sharing Regime: Six Lessons for the World*, No. Forthcoming in King's Law Journal (2021).

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 and internal, enterprise, and external APIs, instead of just focusing on bank-to-customer interactions. The 2018 guidelines for data governance set out detailed architectural structures for the data management of financial institutions.[102] A more recent set of interim provisions stipulate minimum consent and as well as requiring that consent is requested if giving access to third parties.[103] It is emerging as a mandatory system albeit with data as a common resource rather than one controlled by individuals or financial institutions.

Likewise, India is developing yet another Open Banking strategy, one based on individual control of data (as in the EU, UK and Australia) but with its use facilitated via a system of aggregation via licensed data aggregators:[104] In India, Open Banking follows a data aggregator model. Firms licensed by the Reserve Bank of India act as fiduciaries, collecting customer's financial data and sharing it with their consent to third parties.[105] Following the objectives of financial inclusion and facilitating financial competition in the market, account aggregators are a public good that ensures a level playing field, precluding the accrual and appropriation of data management costs by individual institutions whilst allowing reciprocal data sharing.[106] Through aggregate banking, the goal is to extend the India Stack from payments into credit, personal finance, wealth management, and insurance.

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

IV. Emerging Financial Data Governance Strategies

General data governance styles interact with financial regulation in the financial data governance model of any given jurisdiction. The main footprint left by each data governance style onto the financial data governance model pertains to the

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

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

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

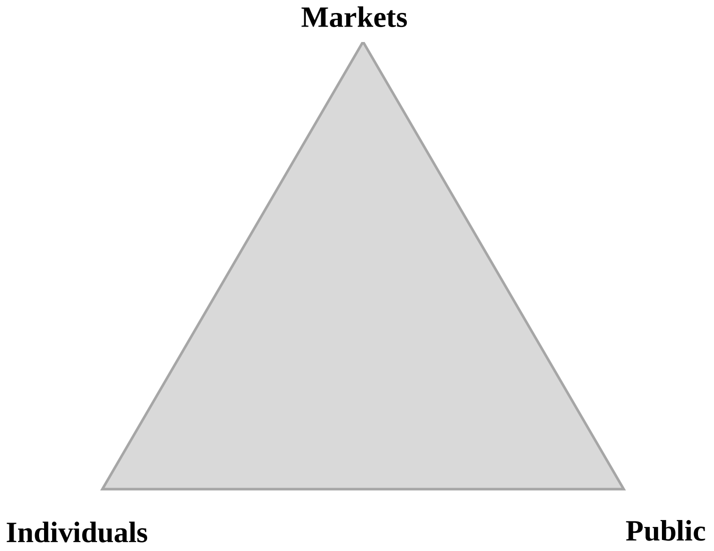
[105] Nandan Nilekani, *Data to the People: India's Inclusive Internet*, 97 FOREIGN AFF. 19 (2018).

[106] Carrière-Swallow et al., *supra* note 103.

attribution of different degrees of control over data to one category of the societal actors populating the data ecosystem. The control over data, in general, and financial data, more specifically, is attributed by prioritizing (i) market dynamics, where data holders, such as business organizations and financial institutions, are key players; (ii) the interests of individuals, intended primarily as the data generators; or (iii) the public interests, representing the collectivity organized by state-actors and public entities.

Through this prism, we identify three archetypical data governance models, based on which group of social actors is prioritized. In market-focused models, control over data is attributed to market dynamics. 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's rights-focused models, control over data is attributed to the individuals generating such data. From a policy standpoint, protection to consumers and data generators tend to be preferred over market dynamics, prompting the adoption of regulatory intervention to curb excessive private powers. Finally, in public-focused models, data is conceived as a collective resource. This style entails a public authority governing the gathering and the use of data through mandatory rules that leave a limited room for interpretation when applied by market participants.

Figure 1: Data Control Concentration Triangle



These archetypes extend to financial data governance. In particular, the different levels of control attributed to societal actors over data influences the regulation of financial data and intersects with Open Banking policies. These three models are analyzed next. First, the market-based model is analyzed as it represents the status quo that favored the development of the data economy and the Internet. The analysis, then, moves to the individual rights-based and the public-centered models, which largely developed to curb an excessive concentration of power accumulated by private entities, primarily based in the US and in China. Examples from the regulatory policies adopted in China, EU, India, and the US.

A. Market-based Models

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

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

The lead in establishing standards for Open Banking products and services is taken by the industry. The Clearing House – a banking association responsible for core payments system infrastructure in the US –[107] has proposed a Model Agreement standard created for data sharing between financial service providers. The aim is to transition from screen-scraping to APIs. A more technical set of standards has been established by the Financial Data Exchange – a cross-section of banks, data aggregators and technology companies created in 2018. These standards create an interoperable API for user-permissioned financial data sharing with over 600 financial data elements currently available, including banking, tax, insurance, and investment data.[108]

While the US may be seen as the clearest example of the ideal of a market-based model for financial data governance, in reality financial regulation in the US – as highlighted above – has long addressed consumer protection in the context of financial data. The US thus is can thus be seen as the leading example of a market-based based of general data governance; however, in the context of financial data governance, it has developed a range of personal and other financial data rules designed to support market efficiency, consumer protection and financial stability.

More recently, these frameworks of consumer financial data protection embedded in the Fair Credit Act in particular are being 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 designed to facilitate data access and use. For instance, in October 2020, the CFPB issued an advance notice of proposed

[107] The Clearing House is owned by the largest banks of the US and has a daily clearing and settlement volume of two trillion US dollars. *See* The Clearing House, *Our History*, https://www.theclearinghouse.org/about/history (last visited Jan. 9, 2022).

[108] Financial Data Exchange, *Home*, FINANCIAL DATA EXCHANGE, https://financialdataexchange.org/FDX/Home/FDX/Default.aspx?hkey=bd839735-ebf5-426a-91f9-8334cbae1438 (last visited Jan. 9, 2022); Oana Ifrim, *The State of Open Banking and Open Finance in the US and Canada – Interview with FDX (Part 1)*, THE PAYPERS, https://thepaypers.com/interviews/the-state-of-open-banking-and-open-finance-in-the-us-and-canada-interview-with-fdx-part-1--1253761 (last visited Jan. 9, 2022).

rulemaking (ANPR) addressing Section 1033 of the Dodd-Frank Act. 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 implementing rules.[109] The Dodd-Frank Act definition of "consumer" is not limited to an individual, but it includes a representative acting on an individual's behalf.[110] The ANPR, however, only outlined principles that may be important to safeguard consumer interests without any prescriptive stipulations. Hence, though industry standards like the Model Agreement aims to incorporate the CFPB Principles, as a template reference they are open to any changes between signatories or in the application of the principles.[111] On this basis, we term the overarching approach to open banking in the US "contract banking," whereby the level of access an individual can provide for a third party to their account information depends in large part on the bilateral agreement between the individual and financial service provider.[112]

The contract banking standard is coming under question by the Biden administration. Until recently, US laws governing data collection and use focused almost exclusively on protecting consumers from harm arising from unauthorized access and inappropriate uses of their data. Highlighting a competition from the consolidation of two thirds of all US banks into the remaining third (and no formal denial of even a single bank merger application in the past 15 years), an executive order was issued.[113] The order directs the CFPB to finalize work to allow consumers and small businesses to "more easily switch financial institutions and use new, innovative financial products."[114] While no new rules have yet 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 US will be whether is sectorally-based approach to data access and use will be effective in the face of its more general data governance style or whether the US will have to generalize the approach of portability being implemented more broadly, as has been done in California and which is being discussed at the federal level. Much depends on the role data itself takes at a federal

[109] 12 USC. § 1033(a).

[110] 12 USC. § 5481(4).

[111] The Clearing House, *Value and Benefit of Model Data Access Agreement*.

[112] The "contractual" relationship with between data stakeholders in the US has also been commented on elsewhere, *See* Bridget A. Fahey, *Data Federalism*, 135 HARVARD LAW REVIEW (2022) (presenting the exchange of data between public entities in the US asa horizontally contractual, rather than top-down organized flow).

[113] Jeremy C. Kress, *Modernizing Bank Merger Review*, 37 YALE J. ON REG. 435 (2020) (outlining how the lax attitude by US regulator towards bank mergers created the "too big to fail" problem and continue to create "too big to jail" and "too big to supervise" issues); Federal Reserve Bank of St.Louis, *Commercial Banks in the U.S.* (2021).

[114] The White House, *Executive Order on Promoting Competition in the American Economy* (2021).

level, where "cross-governmental bureaucracies" – the complex system of informal and formal rules on data flows at the public level, remains largely unregulated and independent of the constitutional federal system.[115]

B. Individual Rights-based Models

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

This model is epitomized by the approach adopted in the EU. The general data governance framework of the Union has evolved around three core priorities: (i) a focus on individual rights and privacy; (ii) the prevention of data concentration in the hands of a handful of dominant firms; and more recently (iii) the promotion of sufficient technological capacity to promote the growth of the internal market. Starting with a series of data protection and privacy directives primarily focused on protecting consumers (EU citizens), the data governance framework expanded in scope and influence.[116] Most recently, both GDPR and PSD2 adopted a series of measures granting ownership and control of data to individuals.[117] The trajectory is posed to be maintained and reinforced with the EU-wide digital ID regime via the eIDAS regulation, which establishes a framework for digital access to cross-border public and private services in the internal market.

[115] Bridget A. Fahey, *Data Federalism*, 135 HARVARD LAW REVIEW (2022)(presenting a case for the structure underlying data pools in US intergovernmental data exchange).

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

[117] Article 36 of PSD2 requires member states "…ensure that payment institutions have access to credit institutions'' payment accounts services….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 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/1 1O/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing 2007/64/EC, 2015 O.J. (L 337) 35, known as PSD2; In turn, Article 20 GDPR provides the right of data subjects to "…receive the personal data concerning him or her" from, data controllers. See EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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), OJ 2016 L119/1.

In this context, different regulatory regimes apply to non-personal and personal data. Non-personal data is generally alienable and can circulate freely.[118] Domestic authorities must be able to retain access to certain data even if located in different Member States and data holders must implement measures to facilitate data portability procedures between service providers.[119] A different regime applies to personal data, which are inalienable from the individual they pertain to and regardless of any contractual agreement.[120] GDPR allows personal data to be exported, subject to the official recognition from the European Commission that the regulatory framework of the receiving (non-EU) jurisdiction ensures basic protection that are deemed equal to those applied in the EU.[121] Furthermore, Member States can enact data localization measures, in the context of health, financial services, or other sectors.[122]

The allocation of control over data to individuals is a pillar of this system. In open banking strategy, individuals maintain control over their data, as financial institutions can share them with authorized third parties only if requested by customers.[123] Yet, financial institutions must ensure that the transfer of data can occur in a systematized fashion and in compliance with a set of minimum requirements.[124]

Built on this framework, the 2020 EU Digital Finance Strategy aims to create a digital Single Market to boost the scalability and competition between financial

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

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

[120] Article 17 grants the “right to be forgotten” by allowing data subjects to – with certain limitations – require data controllers to erase personal data concerning them if the data are no longer necessary in relation to the purpose for which they were collected, thus providing data subjects with the tools to essentially break contracts to secure data rights. See See EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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), OJ 2016 L119/1.

[121] Id.

[122] Id. See Nigel Cory et al., *Principles and Policies for “Data Free Flow With Trust”* (Information Technology and Innovation Foundation 2019) (highlighting the limits of data protection under the GDPR); Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?* (2017) (highlighting the transaction costs of data protection regimes).

[123] Article 64 of PSD2 expressly requires authorization of payment transactions to be considered only if the “payer has given consent to execute the payment transaction.” See Infra at 113.

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

service providers. [125] This strategy includes enabling EU-wide interoperable use of digital identities to allow easier on-boarding, suitability assessments, and the "re-use" of on-boarding for other purposes beyond financial services. This data space will be centered on a new EU digital finance platform that enables industry and supervisory authorities to interact online, offering e-licensing procedures on the basis of the expanded on-boarding regimes and data exchange.[126] One of the key strategies of the 2020 EU DFS is moving from "Open Banking" of PSD2 and GDPR to "Open Finance" in which all financial data must be freely transferable to third parties and eventually under the new EU Digital Strategy, moving to "Open Data", in which data are fully under individual control with the necessary standards and infrastructure to enable use.

The challenge is likely not to be the legal framework: it is relatively simple to define from a legal standpoint that data is a right subject to individual control and to require firms to facilitate this. It is much more difficult to build the necessary technological infrastructure to enable actual control and sharing to enable the ideal of Open Banking / Open Finance / Open Data. While a range of jurisdictions are following the EU's legal approach, the biggest challenge in most will be building the necessary technological infrastructure to make it actually work in practice. The EU is likely to be well-placed to make this happen, particularly in the context of finance, as we discuss in Section 6.

C. Public-focused Models

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

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

[126] Id. LUÍS CABRAL ET AL

China is most emblematic case of a jurisdiction that is implementing a public-focused model. Characterized by a State-centric structure, the emergence of an internal market for data occurs having in view the interest of the collectivity. Following the overarching developmental goal, enshrined in the notion of Common Prosperity,[127] data governance policy pursues a twofold objective. First, the recent emergence of a data governance framework is intended to pursue stability for social, economic, and financial purposes, while maintaining national security. Second, data policies aim at bolstering and supporting the competitive dynamics to promote innovation, through the development of an internal digital market.[128]

This twofold objective results in public-private relationships that evolved in a co-dependent manner. While prior to 2020, data was largely treated in a way that was functionally similar to the US approach, whereby a small number of large firms gathered and traded data on consumers behavior,[129] the central control to curb excessive accumulation of power in private hands became more dominant with a series of legislative and policy interventions.[130] Furthermore, over the past decade, the domestic market was largely protected from foreign competition. This combination of factors led to the development of national champions, such as Alibaba, Weibo, Baidu, and QQ, technical mechanisms to block data inflows and outflows, and institutional capacity for the central government to monitor a vast amount of data.[131] flows and access data for the purpose of pursuing general stability and innovation goals. The result is that the data circulating domestically amount to almost a third of global movements.[132]

In the past years, a "cyber sovereignty" framework has been developed and gradually enacted to promote innovation under a State-centric framework. The

[127] The "Common Prosperity" agenda was set in a variety of speeches by Chinese leadership, focusing on supporting an open and integrated global economy. See CCCPC (Central Committee of the Communist Party of China) and SCC (State Council of China), 2021, " 14th Five-Year Plan (2021–2025) for National Economic and Social Development and the Long-Range Objectives through the Year 2035"

[128] Rogier Creemers, *China's Conception of Cyber Sovereignty*, GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY 107 in GOVERNING CYBERSPACE: BEHAVIOR, POWER, AND DIPLOMACY (D. Broeders & Bibi van den Berg eds., 2020) (discussing the overarching goals of Chinese data governance policy).

[129] Creemers, *supra* note 131.

[130] Together, the the 2017 Cybersecurity law, 2021 Data Security Law, and 2021 Personal Information Protection Law limit private company dominance of data. See supra note 129.

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

[132] Aho and Duffield, *supra* note 21; Wei Yin, *A comparison of the US and EU regulatory responses to China's state capitalism: implication, issue and direction*, 19 ASIA EUR J 1–25 (2021) (discussing the size of China's state-centric form of capitalism).

central pillars of this framework are three fundamental laws: the 2017 Cybersecurity law, 2021 Data Security Law, and 2021 Personal Information Protection Law (PIPL). The overall approach is reflected in a new State Council policy framework enacted in August 2021.[133] While control over data under the emerging system follows an individual-based model, similar to the one deployed in the EU – whereby personal data are inalienable and non-personal data can be freely disposed – ultimate control over data belongs to the central government. Not only does the government have access to data, it also mandates data collection and analysis in both the public and private sector, with a focus on enhancing the Social Credit Score as a central mechanism for monitoring. Moreover, although the government allows uninhibited flows internally, data can only leave or enter China with express government permission.[134]

This state-based data governance style extends to a shared banking paradigm and in fact has been implemented most directly in this context, with a series of regulatory interventions triggered by concerns about Ant Financial leading to a related series of regulatory changes specifically targeting Ant in some cases, addressing the financial sector more generally in others, and in some addressing data and cybersecurity requirements more generally. Financial data is treated as a public resource, under the control of the central government. The largest Chinese digital platforms and BigTechs are entrusted to gather data that feed into the users' social credit score and other credit, commercial and financial scoring systems, both public and proprietary. For this purpose data generated from dispute resolution cases, contract fulfilment, and other financial activities contribute to determine these various credit scores.[135] WeChat – an omnichannel platform with 1 billion active users owned by Tencent – feeds the information back to the Chinese government to build personalized emotional, behavioral, and physiological data and add to user health portfolios.[136] Similarly, the Chinese authorities have

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

[134] Angela Huyue Zhang, *Agility Over Stability: China's Great Reversal in Regulating the Platform Economy*, University of Hong Kong Faculty of Law Research Paper No. 2021/36 (2021) (highlighting China's expanding regulatory oversight via antitrust, financial, and data regulation); Hermes et al., *supra* note 101.

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

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

provided express lists of essential and non-essential data that financial service providers can request from users.[137] More profoundly, with a recent regulatory intervention, the People's Bank of China together with other financial supervisory authorities, ordered 13 of the largest technology firms to unbundle and restructure their business in order to separate the internet-based activities from financial activities; to the undertake the latter type of activities a license is required.[138] As a result, financial services developed to support the data economy are brought squarely within the financial regulation perimeter to "break [the] information monopoly" and "enhance the sense of social responsibility."[139]

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

D. Hybrid Models

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

As jurisdictions may adopt different approaches to allocate control over data, depending on domestic political, legal, and economic idiosyncrasies, hybrid models emerge. The examples offered by China, the EU, and the US are naturally a point of reference, not the least because the US represented the status quo of the global

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

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

[139] *Id.* (the 13 firms include Tencent, Du Xiaoman Financial, JD Finance, ByteDance, Meituan Finance, DiDi Finance, Lufax, Airstar Digital Technology, 360 DigiTech, Sina Finance, Suning Finance, Gome Finance and Ctrip Finance.).

internet governance and the dominant proponent of market-based global finance (although this too has been highly constrained by evolving financial regulation over decades particularly after the 2008 financial crisis and with the development of a consensus-based global regulatory framework very unlike the context of US data companies more generally), the EU has been a first mover in shaping the governance of data and the leader in Open Banking (including its expansion to a broader financial data governance strategy reflected in its broader data governance style), and China is emerging as strong alternative in seeking to develop an increasingly autonomous approach both to data generally and – as illustrated with new financial data strategies and interventions addressing companies including Ant and Didi as well as in the context of developing its digital currency, the eCNY – specifically in the context of an emerging financial data governance strategy, likewise leading in many ways the evolution of its wider general data governance style.

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

The Indian data governance approach reflects a hybrid model that prioritizes the allocation of control to individuals and the state. At the heart of this model is the need to increase financial and public services inclusion through digitalization, combined with a rights based systems for data and combined with a general market framework.[140]

Over the past ten years, India has introduced the multi-layered digital infrastructure known as the "India Stack." India Stack is a strategy designed to put in place infrastructure to enable wider development, innovation and digitalization across India. It consists of a range of APIs, open standards and infrastructure standards that enable access to a broad range of services digitally for Indian citizens.[141] Since 2011, over 90 percent of the Indian population has received a digital identity, and more than half of the identity holders have linked bank accounts to it.[142]

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

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

[141] Yan Carrière-Swallow et al., *India's Approach to Open Banking: Some Implications for Financial Inclusion*, No. WP/21/52 (2021)(describing the development of the India Stack and noting the upcoming "consent layer" as a further enabler of financial data governance).

[142] *Id.*

demographic information. The second layer consists of the Unified Payments Interface (UPI), an API-based interoperable payments interface that can be used by banks and vendors to send money between financial service providers.[143] 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.[144] The last layer is the consent layer, which enables the active management of individual's data through regulated intermediaries. The government has established, for instance, a voluntary standard consent-providing template that enterprises must use to replace opaque and unclear terms and conditions.[145]

The general financial inclusion ethos dovetails with the objective of promoting competition within the domestic financial sector.[146] The Indian financial landscape is dominated by state-owned banks, holding almost two-thirds of total banking assets.[147] By increasing ease of access to financial services – especially in cashless format – competition within its banking sector is expected to increase.[148]

The resulting hybrid model reflects a strong concentration of control over data infrastructure for broader economic, financial and developmental purposes. Yet, the powers of state actors are curtailed within the Indian constitutional framework and India's approach to personal data embodied in a bill expected to be enacted in the near future.[149] In this regard, the Supreme Court decided that Aadhaar identities can be required to receive welfare benefits,[150] while also finding that mandatory linking of Aadhaar accounts is generally unconstitutional with limited exceptions.[151] Banks, for example, are not allowed to deny service if the customer has no linked Aadhaar number.[152]

Attention to the interest of individuals is also a key priority, while market dynamics are favored. India's market so far is a major competitive ground between domestic,

[143] Nilekani, *supra* note 108.

[144] Carrière-Swallow et al., *supra* note 103.

[145] Nilekani, *supra* note 108.

[146] Reserve Bank of India, *National Strategy for Financial Inclusion* (2019).

[147] Id.

[148] Carrière-Swallow et al., *supra* note 103.

[149] Alpha law, *Update On Data Protection Law*, https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law (last visited Feb. 12, 2022).

[150] Utkash Anand, *4-1 Verdict: Supreme Court Dismisses Pleas Seeking Aadhaar Ruling Review*, HINDUSTAN TIMES, https://www.hindustantimes.com/india-news/41-verdict-supreme-court-dismisses-pleas-seeking-aadhaar-ruling-review-101611189869910.html (last visited Jan. 10, 2022).

[151] Ananya Bhattacharya Anand Nupur, *Aadhaar is Voluntary—but Millions of Indians Are Already Trapped*, QUARTZ, https://qz.com/india/1351263/supreme-court-verdict-how-indias-aadhaar-id-became-mandatory/ (last visited Jan. 10, 2022).

[152] *Id.*

foreign and foreign-invested firms, including telecoms, payments, ecommerce, FinTech and a range of financial incumbents.[153] Hence, in a way that is more akin to a market-based model, these companies all share benefit of utilizing the India Stack, while competing for services. Moreover, the recently adopted Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules increase the accountability of social media platforms and empower users of social media platforms through a redressal mechanism requiring a procedure for reporting and removing content.[154]

This general trend is reflected also in India's Open Banking strategy, based on account aggregators, whereby financial institutions are mandated to collect data and shared them with third party. In this context, financial institutions act as fiduciaries to source data,[155] but they may not access, store, or further sell the acquired data.[156] Account Aggregators authenticate subjects using their Aadhaar ID and map the ID to the available documents in the third layer of the India Stack, gaining access and retrieving the subject's financial assets, liabilities, or cashflows.[157] Through these systems, the enable broader financial service origination, underwriting, disbursement and payments.[158]

Through Account Aggregators, India is seeking to provide an interoperable data standard. The operational framework extends data sharing to more classes of data than other jurisdictions, lending availability to any data held in the India Stack. The broader aggregate banking approach is also not limited to the relationship between financial services providers and natural persons – the India Stack data is used also by and for legal persons, with no categorical distinction. However, there is no

[153] 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". Ministry of Electronics & IT, *Government Blocks 118 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order* (2020).

[154] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, *The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules* (2021).

[155] Account aggregators are defined under Section 3 of the Reserve Bank of India Act as a "non-banking financial company…that undertakes 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 Directions regarding Registration and Operations of NBFC - Account Aggregators under section 45-IA of the Reserve Bank of India Act, 1934

[156] Id.

[157] Id.

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

expectation to extend the notion of data aggregators to other areas like search and social media businesses.[159]

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

[159] Carrière-Swallow et al., *supra* note 103.

Table 1: Financial Data Governance Models[163]

Models	Jurisdiction	Open banking type	Participation	Digital-ID scheme	API standardization	Data sharing reciprocity
Market	US	Data portability	Voluntary (upon request of customers)	No	No	Voluntary
Individual	EU	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, non-banks may participate voluntarily

Source: Authors' research and Yan Carrière-Swallow et al., *India's Approach to Open Banking: Some Implications for Financial Inclusion*, No. WP/21/52 (2021).

These emerging financial data governance models depict an international landscape that is increasingly localized particularly for personal financial data. Reflecting the trend observed in the context of general data governance styles,[164] fragmentation is steering the global data governance framework away from the traditional market-led approach which has underpinned the re-emergence of global finance in tandem with digitization since the 1970s.[165] This trend is particularly evident in the context of financial data that are categorized as "personal" under domestic laws but is also increasingly impacting other forms of financial data.

[163] For an analysis of the variables in the table see Arner et al., *supra* note 11; Carrière-Swallow et al., *supra* note 103..

[164] See supra Section III B for a discussion of localization and other trends related to data governance styles.

[165] See supra Section II for a discussion of the evolution of digital, and globalized finance.

V. Challenging the Globalization of Finance?

The intersection between data, finance, law and regulation is not always harmonious. Financial data governance engenders potential conflicts between its core components. Finance is one of the most highly regulated industries, with complex networks of rules addressing financial stability, market integrity, market efficiency, and consumer protection.[166] A dense soft-law architecture ensures a minimum level of international coordination, with overarching policy objectives set by the Group of 20 and standards set by transnational regulatory bodies, such as the BCBS and the FSB.[167] While the regulatory framework for financial data and the emergence of Open Banking initiatives tend to coexist cohesively with financial regulatory policies, the expansion of domestic data governance styles aimed at asserting jurisdictional sovereignty over data, their flows, and infrastructure creates new – at times incongruous – regulatory challenges.

This Section examines three areas of financial data governance where such challenges are most clear. First, we highlight the need for coordination in circumstances where financial data fall concomitantly in the purview of different legal and regulatory branches. This has been most direct in the context of market integrity. Second, the factors underlying data governance fragmentation in particularly geopolitical and competitiveness issues are also increasingly impacting financial data governance and the globalization of digital finance. These forces are compounded by concerns for financial stability. The needs of financial regulation itself is driving localization of data particularly from the standpoint of financial stability but this localization – while seeking to enhance domestic financial stability – may in fact harm global financial stability as the result of the challenges for ensuring an internationally coordinated supervision of financial services. In addition to the changes of data localization for the financial industry, financial data fragmentation raises challenges from the standpoint of the opportunities it creates from gaps and the potential for regulatory arbitrage: blinds spots resulting from the limitations on data access.

[166] DOUGLAS W ARNER, FINANCIAL STABILITY, ECONOMIC GROWTH, AND THE ROLE OF LAW (2007).

[167] The policy direction of financial regulation is established primarily within the group of seven (G7) and the group of twenty G20 most industrialized nations. The direction established in these fora sets the mandate for transnational regulatory bodies. 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 (2019)(describing generally the role of the G7 and G20 in setting core policy directions for international organizations, and discussing how other organizations like the EU participate in the process).

A. Regulatory Fragmentation

To examine regulatory fragmentation and the need for coordination of approaches to financial data, we draw from and expand upon the theory of CLI.[168] Data governance rules do not pertain strictly to commercial law, in general, or to financial regulation, more specifically.[169] Generally, data governance encompasses a variety of rules, legal and regulatory regimes, that – depending on the domestic style – cover how data is created, classified, collected, processed, and used for the purpose of reaching sectoral policy aims.[170] Differently, the regulatory regimes pertaining to the digitization and the datafication of finance are central to financial regulation in the context of digital financial transformation. Yet, the convergence of these branches into the emerging area of financial data governance presents similar dynamics to those observed in the CLI context, where multiple legal rules apply concomitantly and lack of coordination generates tensions and frictions, labelled as "coordination failures."[171]

In the context of financial data governance, coordination failures can take place at two different levels. At the first level, conflicts pertain to the policy objectives of

[168] The CLI phenomenon is ubiquitous and has been identified in Giuliano G. Castellano & Andrea Tosato, *Commercial Law Intersections*, 72 HASTINGS L.J. 999 (2020) (offering an analytical framework to examine CLI and devising a normative approach to address the issues emerging from the lack of coordination in CLIs).

[169] In American legal scholarship, commercial law is traditionally understood as "the body of rules regulating commerce", which include "the laws governing individuals engaged in the manufacture and distribution of objects" as well as "the laws regulating the association of capital", see Layton B. Register, *The Dual System of Civil and Commercial Law*, 61 U. Pa. L. Rev. 240, 241, 244 (1913).

[170] See supra Section III B for a discussion of localization and other trends related to data governance styles.

[171] Scholars have repeatedly emphasized the need for a better coordination between branches of commercial law; *see generally* Catherine Walsh, *The Role of Party Autonomy in Determining the Third-Party Effects of Assignments: Of "Secret Laws" and "Secret Liens,"* 81 LAW AND CONTEMPORARY PROBLEMS 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, 1418 (2007 (denouncing the complexities of the intersections of corporate law, securities regulation, and accounting). International organizations have indicated coordination issues as problematic; see, e.g., UNCITRAL, *Draft Legislative Guide On Secured Transactions*, 65 (2019) at 9 (indicating that the applicability of secured transactions law in a given legal system might be restricted by other laws).

financial and data regulation.[172] This is to say that at least one of the policy aims of data regulation, such as cybersecurity or privacy of individuals,[173] is at odds (or largely incompatible) with one or more of the policy objectives of financial regulation, such as financial stability, market fairness and consumer protection or efficiency.[174] The second level of conflictual relationships comprises contrasts that, while not involving policy objectives, result in incongruencies between dispositive rules and principles,[175] such as those establishing the non-alienability of personal data, or operative prepositions,[176] like the rules regulating APIs or the format and modes in which customers data must be collected.[177]

An example of a coordination failure of the first level involves the frictions between privacy objectives, prudential rules, and efficiency and transparency of payment systems. In cash payments, there is an innate element of full privacy, owing to the inherent anonymity of cash-based transactions. However, such a degree of anonymity, which is a rich ground for money laundering activities, is not a feature of DLT payments.[178] In the context of central bank digital currencies (CBDCs), while anonymity (at least vis-à-vis regulators and enforcement authorities) is not

[172] Policy aims formulate the ordering criteria and shape the development of each law branch. These policy aims may be extrapolated from a range of diverse sources including statutes, regulatory principles, or case law. See Castellano & Tosato, *supra* note 21.

[173] In the US, the right to privacy has been enshrined in the Privacy Act, which stringently regulates how the US government collects data about individuals. See 5 U.S.C. § 552a; In the EU, the respect for private and family life and protection of personal data are a fundamental right enshrined in the European Charter of Fundamental Rights, see Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C364) 1. Discussions on the interpretation of data privacy are also seeing growing academic discussion. See Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARVARD LAW REVIEW (2021)(presenting an argument in favor of deleveraging the doctrine of using Stored Communications Act to bar subpoeanaing the contents of other's online communication in a criminal defense).

[174] This is considered a Multi-core CLI coordination failure – one which is characterized by gaps or incongruences that stem from tension between the core spheres of two or more of the converging legal branches, see Castellano & Tosato, *supra* note 21.

[175] 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.*

[176] Operative propositions indicate the rules and principles that fall within the system of rules and principles and doctrines underlying key tenets of a law branch. See *Id.*

[177] For example, PSD2 requires the European Banking Authority to develop regulatory technical standards setting technical requirements to be used by payment service providers. See infra note 113 Art 98

[178] Rodney J. Garratt & Maarten RC Van Oordt, *Privacy as a Public Good: A Case for Electronic Cash*, 129 JOURNAL OF POLITICAL ECONOMY 2157 (2021)(arguing that with the disappearance of cash, the digitalized transactions are the intermediaries of digital payments with information that can skew the market).

an option, the protection of privacy is critical in many societal contexts.[179] As a public good, privacy is important to ensure a variety of outcomes, from preventing data-based price discrimination,[180] to ensure democratic functions.[181] For this reason, different forms of privacy measures have been considered, including regulatory techniques like government access based solely on issuance of a warrant, or cryptographic methods that automate pseudo-anonymization.[182] Nonetheless, each option requires a compromise, or a trade-off, between policy objectives.[183] A prioritization of privacy objectives will necessarily result in a subordination of financial regulation policies, aiming at ensuring the integrity, fairness, and efficiency of financial markets. In a similar vein, the sole pursuit of financial regulation policies would imply to lessen privacy protections. In the context of CBDCs, this is likely to result in a range of different structures reflecting differing balances of societal objectives.

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

The international regulatory framework for AML focuses on the role of intermediaries (particularly financial intermediaries such as banks) and law enforcement agencies in collecting data to ensure compliance. AML measures by financial institutions are managed via a risk-based assessment (RBA) framework,

[179] Ellie Rennie & Stacey Steele, *Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency*, 3 LAW, TECHNOLOGY AND HUMANS 6 (2021)(discussing the variety of methods to approach ensuring privacy in a trend of phasing out of cash and replacing it with digital payment instruments).

[180] Supra note 171

[181] Bilyana Petkova, *Privacy as Europe's First Amendment*, 25 EUROPEAN LAW JOURNAL 140 (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).

[182] See supra note 172.

[183] Trade-offs require a prioritization of the policy aims of one branch over those of another. See Castellano & Tosato, *supra* note 21.

as set by the main international AML standard-setting body – the Financial Action Task Force. Under the RBA, each financial services provider must create risk profiles for their clients, products, correspondent banks, and other parts of the financial service supply chain. These profiles feed off data that the bank must collect through its own sources, from B2B services, its own affiliates, or other sources. Law enforcement and financial intelligence agencies will likewise develop similar profiles.

An issue with dispositive rules and AML has emerged particularly in the context of Open Banking rules, most dramatically in the EU. Open Banking is a function of retail consumer ownership and/or control of their financial data. This ownership and/or control entails classifying an array of types of information, including creditworthiness, customer preferences, but also transaction histories. In the EU, PSD2 – which mandates the Open Banking regime – provides a level of data protection for personal data, with an exception for processing personal data by obliged entities when "necessary to safeguard the prevention, investigation and detection of payment fraud."[184] However, a later law, GDPR, establishes a higher level of data protection that, while providing similar exceptions applies them particularly to processing personal data in "criminal cases," not collection.[185] In 2019, the European Data Protection Service (EDPS) requested the cease of operations of FIU.net – a core tool for the exchange of financial intelligence between Member States operated by Europol – due to a lack of status as criminals.[186] In early 2021, a similar conflict led the EDPS to require Europol to delete huge databases on individuals with no criminal status.[187] Through these direct conflicts in approach, AML supervisors lost access to data to undertake their functions and share with regulated entities to construct in pursuit of their own obligations.

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

[184] See supra note 113 Art 94

[185] See supra note 14 Art 2 (2)(c)

[186] 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 JOURNAL OF EUROPEAN CRIMINAL LAW 351 (2020)(discussing how the financial intelligence units are particularly prone to data protection issues in the EU because of their - at times - administrative entity status).

[187] See supra note 13.

evolved in the EU in the context of personal and financial data rules.[188] Financial data governance must seek to balance competing regulatory objectives.

This is also an increasing issue as both financial data governance and general data governance seek to act on an increasingly extraterritorial to territorialize data requirements.

B. Territorialization and Data Localization

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

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

Preferential trade agreements set out express prohibitions on limiting the movement financial data. The EU-Japanese Economic Partnership Agreement, 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.[189] Stipulations like these expressly set financial services as a

[188] See Emilios Avgouleas & Alexandris Seratakis, *Governing the Digital Finance Value Chain in the EU: MIFID II, the Digital Package, and the Large Gaps between*, European Company and Financial Law Review (2021).

[189] Agreement between the European Union and Japan for an Economic Partnership, art. 8.63, July 17, 2018, http://trade.ec.europa.eu/doclib/press/index.cfmid=1684 [hereinafter EU-Japan EPA].

priority, acting as a carte-blanche on the use of financial data for holders, aggregators, and processors depending on the interpretation of the ever evolving characterization of financial services.

A second express priority is for jurisdictions to ensure financial stability and market integrity. To this end free trade agreements have special carve outs enabling data access to financial service providers if necessary for regulating domestic financial markets. The United States-Mexico-Canada agreement (USMCA) recognizes the "immediate, direct, complete, and ongoing access" of regulatory authorities to information that is "critical to financial regulation and supervision." The USMCA further specifies data access for the sake of maintaining market integrity, safety, or financial responsibility.[190]

Following the free-market regulatory style, the USMCA agreement also prohibits requirements on local data storage. However, this prohibition is only applicable in circumstances where the financial regulator has "immediate, direct, complete, and ongoing" access to data that it needs to fulfill its regulatory and supervisory mandate.[191] The lack of necessary access to data relevant for financial supervisory goals can trigger a dispute and, in essence, the data access paradigm is a faux-data localization limitation.

The China-Korea FTA has a similar effect to the USMCA, but from the other perspective. The agreement similarly provides a prudential carve out that allows parties to "adopt measures for prudential reasons."[192] The scope for prudential protection is similarly wide, extending to protecting investors, ensuring financial integrity and stability, among other reasons. However, following the shared-banking principles of China, the agreement contains no limitations on data localization measures. Depending on interpretation, the prudential carve outs of both the USMCA and the China-Korea FTA can provide an equivalent access to the financial data of third-country subjects, irrespective of the other data provisions.

Though there are clauses limiting the disclosure requirements a jurisdiction can enact for financial data, they are relatively minor. All three agreements expressly prohibit parties to disclose information relating to the affairs and accounts of

The USMCA similarly has a provision prohibiting the prevention of data transfer into and out of the territories of the parties, *See* United States-Mexico-Canada Agreement, Can.-Mex.-U.S., art. 17, Nov. 30, 2018, 134 Stat. 11 (2020) [hereinafter USMCA].

[190] Article 9.5 Id

[191] *Id.*

[192] Free Trade Agreement between the Government of the People's Republic of China and the Government of the Republic of Korea, art 9.5, June 1, 2015, http://fta.mofcom.gov.cn/korea/annex/xdzw_en.pdf [hereinafter China-Korea FTA].

particular customers, or any confidential or proprietary information possessed by public entities.[193] However, there is an implied right for financial service providers to transfer personal client information to the servers of other banks across jurisdictions. These are significant divergences from the hard prohibition on personal data transfer from China, or the extraterritorial personal data protection requirement of the GDPR.

Free trade agreements highlight the exceptional nature of financial data. This exceptionalism is being approached on to meet other policy priorities. As cross-fertilization of financial data and broader data governance styles grows, the prior is increasingly entering the ambit of other data-driven priorities. This can take place by embedding financial data into systems under other areas of law, whereby they become integrated and inextricable from other rules, or it can affect financial data directly.

An example of the territorialization of financial data is Open Banking. Open Banking, by mandating certain technical levels of interoperability from banks, via data portability or API standards, integrates client financial data into a broader – usually domestic – data system. These systems, like the India Stack, enable the use of financial service through local Aadhar digital ID, the standardized unified payments interface, and data aggregators and fiduciaries that verify data access rights. Any financial data on the account and transaction of individuals will be fit bound to the India Stack, limiting the movement of financial data through a lack of technical interoperability, as well as the variety of personal data, certification, and other rules protecting the Stack.

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

[193] China-Korea FTA, *supra* note **Error! Bookmark not defined.**, art. 9.4. *See* USMCA, *supra* note **Error! Bookmark not defined.**, art. 17.8; EU-Japan EPA, *supra* note 189, art. 8.65.

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

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

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

C. Data Gaps

The third challenge to the paradigm of global financial flows is tied to the increased opaqueness of the market itself. Global financial stability is underpinned by a complex international system of rules. The development of this soft-law law system has been responsive to the evolving risks to financial stability, bolstering data collection and financial standards in a feedback loop. The Basel Committee was established to after disturbance in international currency markets in the 1970s, and has continued laying bolstering standardization for financial services supervision, with Basel III responding to the 2008 Global Financial Crisis by enhancing higher global minimum capital and risk management requirements.[194] Similarly responsive, are international data collection initiatives, like the IMF Standards for Data Dissemination, that enable the sharing of domestic economic and financial data for the purpose of global macroeconomic, established in 1997 in response to the lack of data pre-empting the Asian financial crisis.[195] Similar well-developed initiatives exist in a range of contexts via the FSB, OECD, IOSCO and other

[194] Basel Committee on Banking Supervision, *History of the Basel Committee* (2014).

[195] Data on government finances, in particular foreign exchange reserves and government debt were found to be severely lacking. *See* THE SPECIAL DATA DISSEMINATION STANDARD: GUIDE FOR SUBSCRIBERS AND USERS (International Monetary Fund ed., 2007).

international financial and regulatory cooperation and standard-setting organizations.

The datafication of financial services is bringing new data gaps; fragmentation of financial data governance via data localization requirements also raises risks of regulatory arbitrage. While international soft law sets a wide range of standards for financial data standardization and regulatory cooperation, in many cases requirements lack sufficient granularity; likewise, despite shared objectives and the well-developed international architecture, geopolitical, national security and competitiveness challenges are increasing. The highly regulated financial regulatory market is made even more dynamic by the datafication process which brings new challenges to regulating and monitoring financial markets. The result is that even as new sources of financial data emerge via new FinTech, RegTech, or other technology-driven digital businesses or tools, their haphazard integration into the existing financial regime may increase opaqueness of markets and create new blind spots for regulators. These blind spots, in turn, can create novel channels for systemic risk.

New data-driven FinTech remains a Wild West for financial regulators. While the supervisory and reporting expectations for traditional banking activities are clear, especially toward the requirements for bank balance sheets and risk management – new digital financial services providers remain uncalibrated. In part, this is due to the growing unbundling of financial services, enabled by digitalization. Virtually the whole bank can be divided into their constituent parts, from origination, intelligence, risk management, to operations, which can then be provided as individual services to businesses and customers or banks themselves.[196] This can include customer facing process 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.[197] Many of these processes can be modularly provided by non-licensed entities, under a variety of licensing regimes with different disclosure and reporting standards.[198]

The differences in regulating FinTech extend to their most basic level of supervision by regulators. The surge of new types of FinTech products and services, and the rise of non-financial enterprises providing these services is resulting in a transnationally divergent approach to classifying, and thus supervising such

[196] Peter Zetterli, *The Great Unbundling* (2021).(discussing how technology is making financial services modular and how it helps inclusion).
[197] *Id.*
[198] 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, 153 (Michael R. King & Richard W. Nesbitt eds., 2020).

services. The example of how a single FinTech entity – in this case PayPal – is beholden to different disclosure and reporting standards across borders portrays how it may be difficult to collect financial data in even one novel market segment.

Under the dual banking system of the US, state law determines the legal status of a financial company. Until now, nonbanks, for example, are not under the purview of federal banking regulators, instead being subject to state regulatory authorities and state law with regards to licensing, examination, reporting requirements, and other consumer protections.[199] PayPal, for example, is not a bank, and is not insured by the Federal Deposit Insurance Corporation and is not subject to a federal prudential regulator. It has a different form of "money transmitter" license in every state.

In the EU, Member States can decide whether or not certain types of institutions can start operating with an initial capital requirement lower than the EUR 5 million traditionally required for banking institutions (Lithuania, for example, has a minimum capital requirement of EUR 1 million for licensing specialized banks).[200] In China, PayPal became the first foreign firm with full ownership of a payment business, thus receiving a payment services license directly from the central bank – the same license issued to WeChat and Alipay.[201] 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 across the jurisdictions of the US, EU, and China, as well as the individual US states. In turn, less and less standardized regulatory data is available on new financial data-driven companies.

At the frontier of FinTech opaqueness are cryptocurrencies. Cryptocurrencies operate under a varied status in different jurisdictions. Depending on their structure, in the US they are considered a substitute for currency, while the EU considers it a crypto-asset. In 2021, China banned owning cryptocurrency, but the EU and US have only placed due-diligence requirements on virtual asset providers.[202] There is no system for truly enforcing and following the vast decentralized finance networks

[199] These issuances have come under significant challenge by stakeholders in Vullo v. Office of the Comptroller of the Currency, 378 F. Supp. 3d 271, 296 (S.D.N.Y. 2019) (the "Vullo Ruling") and Lacewell v. Office of the Comptroller of the Currency, 2019 U.S. Dist. LEXIS 182934 (S.D.N.Y. Oct. 21, 2019).

[200] European Commission, *Interview with Marius Jurgilas*, EUROPEAN COMMISSION, https://ec.europa.eu/newsroom/fisma/items/684838 (last visited Feb. 12, 2022).

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

[202] Notice on Further Preventing and Dealing with the Risk of Speculation in Virtual Currency Transactions, available at https://perma.cc/DC7U-MSDF

that are growing on hundreds of different blockchains. For example, a novel type of secondary financial market is emerging in the domain of non-fungible tokens, where loans taken in a blockchain based decentralized finance network can be sold as non-fungible tokens.[203] The same dynamic already supports prediction markets, swaps, and longs and shorts.[204] Because of the decentralized nature of blockchain, and the different regulatory approaches being taken, tracing these fast-growing markets is virtually impossible.

These challenges in consolidate significant data gaps as well as opportunities for regulatory arbitrage, with systemic implications. The divergence of regulating FinTech, and the difficulty in monitoring their derivative financial data is resulting in a lack of transparency regarding local, and thus international FinTech markets. This includes a lack of understanding of types of operations, counterparties, interest rates, terms, and even the currency (including crypto assets) used in operations. Without this information, it is also difficult to ascertain the size of interrelationships with other financial entities, and their funding and credit exposures by sector.

VI. Addressing the Challenges of Financial Data Governance: Moving beyond the Data Centralization Paradigm

Will financial data territorialization, localization and competition fundamentally challenge financial globalization? Or will data gaps and regulatory arbitrage as a result of financial data localization sow the seeds of the next financial crisis? We suggest that data localization will remain the status quo of financial data for a variety of reasons. It is critical to the fulfilment of policy objectives, it often lacks interoperability with the financial data of other regimes, and the variety of licensing frameworks ensure that even the same entity may be generating 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, provides an avenue to address the most severe risks of conflict and fragmentation.

[203] CDzExchange, *NFTs and the Derivatives Market*, MEDIUM, https://medium.com/cdzexchange/nfts-and-the-derivatives-market-8127ada445df (last visited Feb. 12, 2022).

[204] *Id.*

A. The International Financial Architecture: Addressing New Challenges

Unlike transnational data governance,[205] global finance has a very well-developed framework for international cooperation and coordination. This framework provides a mechanism for cooperation in areas relating to transnational financial data. Existing mechanisms support standardization of disclosure and reporting requirements (essentially the framework for many forms of financial data creation and assurance) as well as cooperation in cross-border enforcement in both market conduct and market integrity, with well-developed cross-border cooperation and information sharing in the contexts of payments, banking, and securities.

In the context of finance different, well-functioning, cooperation mechanisms already exist and can be leveraged to facilitate the circulation of data. For example, an answer to this may lie in the work of 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.[206] Building on Legal Entity Identifiers, Unique Transaction Identifiers (UTI), and Unique Product Identifiers (UPI), reported to trade repositories and authorities, the final list of harmonizable CDE has 110 items that standardize cornerstone information like counterparty, beneficiary, and clearing, trading, and settlement information, but also allows for more granular approaches to collateral, margins, prices, and other details.[207] These elements aim to remain technologically neutral, allowing a range of technological approaches. At the same time, by setting standards for the creation and use of various forms of financial data, they also set the parameters required of the technologies used to create, store, protect, use and transfer data: technological neutrality is often more constrained than portrayed.

[205] Arner et al., *supra* note 8; Institute of International Finance, *Strategic Framework for Digital Economic Cooperation* (2021)(arguing for the need of a new permanent structure to help guide international digital economic cooperation); VIKRAM HAKSAR CARRIERRE-SWALLOW, YAN, GIDDINGS, ANDREW, ISLAM, EMRAN, KAO, KATHLEEN, KOPP, EMANUEL, QUIROS ROMERO, GABRIEL, TOWARD A GLOBAL APPROACH TO DATA IN THE DIGITAL AGE (2021)(presenting a case for global data policy frameworks).

[206] *Harmonisation of Critical OTC Derivatives Data Elements (Other Than UTI and UPI) - Technical Guidance*, BANK FOR INT'L SETTLEMENTS, https://www.bis.org/cpmi/publ/d175.htm (last visited Dec. 1, 2021).

[207] BANK FOR INT'L SETTLEMENTS & INT'L ORG. OF SEC. COMM'N, HARMONISATION OF CRITICAL OTC DERIVATIVES DATA ELEMENTS (OTHER THAN UTI AND UPI) - TECHNICAL GUIDANCE (2018), https://www.bis.org/cpmi/publ/d175.pdf.

More broadly, general initiatives can be concerted at the international level. The G20, via 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, data[208] are increasingly cached on sectoral "deposit-taking corporations" and "other financial corporations" that include novel FinTechs.[209] Thus, more of the available information is used to pursue micro- and macro-prudential data collection through an increasingly harmonized global rulebook that entails the US, EU, and China.

As financial data harmonization increases, an expansion of current disclosure requirements due diligence rules is required. Necessarily, this will result in a more assertive utilization of RegTech and SupTech solutions that are capable of drawing on more timely data, and combining data from a variety of sources to build prudential models about traditional and novel financial services.[210] These systems will increasingly depend on the coordination of several foundational infrastructures (like telecommunications), along with digital and financial infrastructures (like mobile data services, data repositories, and payment and settlement services) to facilitate the collection of data from new sources.

Challenges in financial data will remain. Differences between statistical and supervisory reporting standards (like the 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.[211] New or existing international fora, like the Global Financial Innovation Network, which counts US, many EU member

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

[209] INT'L MONETARY FUND, THE SPECIAL DATA DISSEMINATION STANDARD PLUS: GUIDE FOR ADHERENTS AND USERS (2013), https://www.imf.org/external/pubs/ft/sdds/guide/plus/2013/sddsplus13.pdf.

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

[211] For an example of federated approaches to financial data sharing see Marina Cernov & Teresa Urbano, *Identification of EU Bank Business Models* (European Banking Authority, Research Paper No. 2, 2018), https://op.europa.eu/en/publication-detail/-/publication/da027419-4c80-11ea-b8b7-01aa75ed71a1/language-en/format-PDF.

states, and Chinese authorities as participants,[212] 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,[213] will fracture the existing international financial architecture. The global financial architecture has continued to function more effectively than most other aspects of international cooperation and institutions owing to its continuous evolution. In general, as we have argued elsewhere, for areas beyond finance, a Digital Stability Board similar to the Financial Stability Board would provide an important cooperative mechanism going forward.[214]

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

Perhaps the greatest opportunities however lie in new technologies.

B. Technological Solutions: Moving from Financial Data Centralization to Decentralization

In addition to the harmonization and a reinforced architectural framework supporting financial data governance, the financial sector is uniquely placed to develop technological solutions to the challenges of data localization and territorialization. Different technological systems have been developed.[215] All systems originate from the genesis format.[216] Under this model, the data collector

[212] CHARLES R. TAYLOR ET AL., INSTITUTIONAL ARRANGEMENTS FOR FINTECH REGULATION AND SUPERVISION (2020).
[213] Mark Austen, *Addressing Fragmentation in Asian Markets: Data Localisation – GFMA's Data Privacy, Security and Mobility Principles* (2019); ASIFMA, *Addressing Market Fragmentation Through the Policymaking Lifecycle* (2020)(presenting emerging examples of market fragmentation tied to sustainable finance, data privacy, AML compliance, and operational resilience).
[214] Arner et al., *supra* note 8; Institute of International Finance, *Strategic Framework for Digital Economic Cooperation* (2021)(arguing for the need of a new permanent structure to help guide international digital economic cooperation); VIKRAM HAKSAR CARRIERRE-SWALLOW, YAN, GIDDINGS, ANDREW, ISLAM, EMRAN, KAO, KATHLEEN, KOPP, EMANUEL, QUIROS ROMERO, GABRIEL, TOWARD A GLOBAL APPROACH TO DATA IN THE DIGITAL AGE (2021)(presenting a case for global data policy frameworks).
[215] Bruno Carballa Smichowski, *Alternative Data Governance Models: Moving Beyond One-Size-Fits-All Solutions*, 54 INTERECONOMICS 222 (2019).
[216] *Id.*

has exclusive control over collected data.[217] However, there is an increasing range of variants being offered. Under 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.[218] Trusts would hold data across jurisdictions and offer a variety of risk appetites and management structures, allowing pre-authorized pools of data to be sent to appropriate third parties.[219]

Jurisdictions could agree on pockets of rules for how and what data can be transferred and through which channels. A variety of technologies are already available to help secure such messages, from blockchain applications, to security-by-design solutions that can help guarantee security of transmissions medium, to AI that can rapidly analyze the content of transmitted data. SWIFT, or other systems of payments messaging, or credit card messaging could adopt such a system, for example. The data from local banks could transmit to a central standardized unit that automatically would process whether and where the data is allowed to route through in accordance with agreement by jurisdictions, similarly to how Qualified Trust Service Providers under the EU PSD2 regime certify digital ID certificates by pinging back to domestic authorities. These kinds of pockets will be vital for critical functions like cybersecurity, market integrity, and increasingly – sustainable financing, via technical, trust, and identification requirements for data transfers.

Concurrently, the private sector could facilitate the adoption of new technologies that would lessen regulatory tensions. These technologies use new techniques to reach the outcomes necessary for offering their products and services, without needing to interfere with or even directly access the data of other entities with or across jurisdictions. Federated data systems that divide bundles of data across many different systems can ensure that no party has a data monopoly,[220] whereby cloud data centres can ensure that it is always accessible though cloud infrastructure does

[217] *Id.*

[218] Sylvie Delacroix & Neil D Lawrence, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, 9 INT'L DATA PRIVACY L. 236 (2019).

[219] 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 id.*

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

raise separate financial stability, national security, and competitiveness issues of its own.[221] Through federated data analytics, banks and supervisors may not need to access the data of other parties at all, instead only requesting that they run the necessary portion of data analytics locally. Lastly, zero knowledge proof protocols enable secure responses from federated or decentralized data system without any access to or knowledge of the underlying data.[222] From the standpoint of infrastructure for financial data, blockchain and other decentralized structures therefore offer potential approaches, in particular from the standpoint of networking various data sources and enabling proprietary analytics, but require a change in mindset about the nature and use of financial data.[223]

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

Conclusion

In this paper, we introduce financial data governance. The coalescence, in different forms, of data governance styles, financial regulation, and personal financial data regulation such as Open Banking policies generates a variety of financial data governance models. Through a comparative investigation, four archetypical models are emerging, depending on whether a higher level of protection is given to the interests of market's participants, individuals, or the collectivities. As legal rules and regulatory regimes traditionally separated are coming together, their concomitant application gives rise to a series of new challenges. Specifically, two sets of challenges are most significant.

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

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

[223] Douglas W. Arner et al., *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*, SSRN Electronic Journal (2018).

The first set of challenges is substantive in nature. Financial regulation and data governance sometimes have shared objectives and in other cases potentially conflict, not only as a result of differing core objectives in some cases but also as a result of siloed expert-led development processes that do not consider other aspects. This is the case, for instance, of the clash between privacy rights, lying at the core of many data governance regimes, and transparency needs in the context of financial data regulations, Open Banking, and, more generally, the digitalization of financial services. Drawing from and expanding the notion of CLI, such 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, thus, at the expense of market dynamics, or to the transparency or efficiency of financial transactions, thus, limiting the protection to individual privacy.

The second set of challenges relates to the growing tension between the globalization of finance and fragmentation of data flows. The territorialization of financial data is an effect of the growing focus of nation-states on digital, financial and economic sovereignty. This can be seen in personal financial data, directly affected by the limitations posed by data governance to their circulation, but also in the context of customer and transactions data, required to be stored locally for prudential reasons, and company data, 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 globally systemically important financial institutions.

Our findings suggest that financial data territorialization is likely to increase. The trend might be further reinforced, as the opaqueness of financial flows stemming from new FinTech solutions may reinforced the need to store data where it can be controlled. A multi-layered solution is required in order to facilitate essential cross-border access to financial data and digitalized services.

At the most fundamental level, the harmonization of processes and rules concerning the gathering and transferring of data is required. This approach implies the possibility of 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 lies in taking the technologies of digitization and datafication and using them – by regulators, by industry participants, by individual customers – to address the reality that data can be stored anywhere and that it is not data itself that is the focus but rather the way in which it can be used and this is determined by the application of analytics. New technologies such as cloud and jurisdictionally based data centers as well as blockchain enable data storage and security design 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 storage require new forms of analytics such as federated learning and zero knowledge systems in order 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, law and regulation affecting data will have consequences on the financial system, whereas financial regulation must deal with the digitization and datafication of finance. Second is that policymakers, regulators, and market participants must reconceptualize financial data and financial data analytics, moving away from the rules and processes grounded on centralized control, to pro-actively devise solutions that are grounded in decentralized approaches.