FROM INDUSTRY SANDBOX TO SUPERVISORY CONTROL BOX: RETHINKING THE ROLE OF REGULATORS IN THE ERA OF FINTECH

Cheng-Yun Tsang[*]

ABSTRACT

Rapid developments of financial technology (fintech) and the unbundling of financial services have given rise to greater collaboration between financial institutions and fintech innovators. Such collaboration takes four major forms: Third-party service relationships, data-sharing arrangements, regulatory experiments, and industry consortia. Each type of collaboration presents certain risks or governance issues to the consumers, the participating firms, and the financial market as a whole, and hold different ramifications for the existing regulatory regime. This paper argues that a novel regulatory approach is needed to help the regulators continuously identify, evaluate, and address the issues as these fintech-era collaborations deepen. This paper proposes that with the proper use of supervisory technology (SupTech), regulators can turn current initiatives such as industry sandboxes into the supervisory control boxes to effectively regulate fintech-era collaborations and shift current practices into a new paradigm of technology-enabled regulation.

Table of Contents

[*] Assistant Professor, College of Law, National Chengchi University (NCCU); Director of the FinTech Regulatory Innovation Lab at NCCU's FinTech Research Center. Duke University School of Law S.J.D (2015). This paper was presented at the Comparative Corporate Governance Conference held in Singapore on January 24, 2019. The author appreciates comments and feedbacks from the conference panelists and participants. This paper is supported by the Ministry of Science and Technology of Taiwan (R.O.C) Rsearch Project Grant "The Impacts of the Development and Use of SupTech on Financial Regulation and the Responding Strategies" (108-2410-H-004 -002 -MY2). The author would also like to thank Professor Ross Buckley for his insightful comments, as well as Isaac Ambruso and Eason Lin for their research assistance. The author is also immensely grateful to the two anonymous referees' comments and suggestions, which help the author greatly refine the paper. All responsibility remains with the author. The author can be reached at cytsang@nccu.edu.tw

I. INTRODUCTION

The rise of financial technology (fintech) has transformed modern financial markets and posed unprecedented challenges to the regulators.[1] Firstly, the cost-effectiveness and improved accessibility of innovative information technologies have allowed nonfinancial firms to offer financial services to underserved groups or provide better customer experience to previous clients not satisfied by the incumbent financial institutions.[2] These new market entrants often target certain niche areas and pain points in the value chain of finance and thus do not have to operate as typical financial institutions which offer one-stop-shop solutions for its customers.[3]

Some of the entrants adopt a B2B (Business to Business) model and treat financial institutions as their clients. These firms usually have a contractual relationship with financial institutions and undertake a third-party service provider role to serve the financial institution's customers indirectly. Many market entrants, on the other hand, adopt a B2C (Business to Consumer) model and compete directly with incumbent financial institutions. In this case, the new entrant may still cooperate with the incumbents in certain areas as the niche service it offers can only satisfy part of the

[1] For a comprehensive review of regulatory issues arising from fintech that merit supervisory authorities' attention, *see* FIN. STABILITY BD., FINANCIAL STABILITY IMPLICATIONS FROM FINTECH SUPERVISORY AND REGULATORY -ISSUES THAT MERIT AUTHORITIES' ATTENTION (June 2017);
For a forward-looking overview of fintech and its potential impact on the banking industry and bank supervision, *see* BASEL COMMITTEE ON BANKING SUPERVISION, SOUND PRACTICES: IMPLICATIONS OF FINTECH DEVELOPMENTS FOR BANKS AND BANK SUPERVISORS (Feb. 2018).

[2] *See* U.S DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES NONBANK FINANCIALS, FINTECH, AND INNOVATION 5-6 (July 2018) (noting that "[f]rom 2010 to the third quarter of 2017, more than 3,330 new technology-based firms serving the financial services industry have been founded", and "[t]he nonbank sector has responded opportunistically to the pullback in services and increased regulatory challenges placed on traditional financial institutions.")

[3] For an analysis of how fintech players compete with incumbent financial institutions in the financial services value chain, *see* Mark Carney, The Promise of FinTech – Something New Under the Sun?, Speech at Deutsche Bundesbank G20 conference on Digitising Finance, Financial Inclusion and Financial Literacy, Wiesbaden 4-7 (Jan. 25, 2017).

consumers' needs. Be it a third-party service provider or a direct competitor, increased cooperation with the financial institutions has become a norm for fintech firms and begs the question of whether and what risks would arise from such close collaboration.[4] Such collaboration generally takes the form of a third-party service relationship and will be discussed further later.

Secondly, advanced information technologies such as data analytics and cloud computing have dramatically increased firms' ability and efficiency to collect and analyze data.[5] Consumers leave their digital footprints and metadata everywhere as using mobile devices and social media every hour and moment has become a common lifestyle.[6] In the past, financial institutions rely heavily on processes such as Knowing Your Customers ("KYC") to collect information which helps indicate a customer's willingness and ability to repay a loan and gathers data to help the institution to determine the level of funding cost a customer should enjoy. In other words, financial institutions generate profits by making sense of their customers' data.

This model, however, is no longer a financial institution's privilege. Many nonfinancial firms such as telecommunication companies, e-commerce platforms, social media, and retail corporations now have more data than their financial counterparts and can also use the data to identify a customers' financial needs and determine his or her creditworthiness.[7] The availability and accessibility of diversified sources of data allow firms to have better insight into the market[8] and offer financial solutions that may seamlessly fit customers' needs. The rise of such data-enabled finance puts customers' data privacy and security at risk too. Financial institutions traditionally are held to the highest standard when it comes to the protection of customers' data. But this does not seem to be the case for nonfinancial firms if we refer to the incredible scale of data leaks recently suffered by some big techs and retail giants.[9]

---

[4] *See* Michal Gromek, *Why Banks and FinTech Need Each Other... And For How Long*, FORBES, July, 19, 2018, available at https://www.forbes.com/sites/michalgromek/2018/07/19/why-banks-and-fintech-need-each-other-and-for-how-long/#6e496c091345 (last visited Jan. 10, 2019) (explaining why fintech innovators would want to cooperate with banks.)

[5] Jeremy Rudin, Data Science and the Future of Financial Supervision, Remark to the 11th Symposium on Asian Banking and Finance, San Francisco, California 1 (June 25, 2018) (stating that "[w]e have all seen how technological change is reshaping the financial services industry. To my mind, the most important of these developments is the remarkable explosion in our ability to collect and analyze data. The data sets available now are so large that they call for new approaches to analyzing them; approaches that harness the continuing growth of computational power by using machine learning and artificial intelligence more generally.")

[6] *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 13 -23 (2015, 1st Edition) (explaining how data has become a by-product of computing and how metadata can be used to enable effective surveillance.)

[7] For example, Alibaba's affiliate - Ant Financial in 2015 introduced its credit-scoring service Sesame Credit based on online and offline data to generate individual credit scores for consumers and small business owners. *Ant Financial Unveils China's First Credit-Scoring System Using Online Data*, BusinessWire, Jan 27, 2105, available at https://www.businesswire.com/news/home/20150127006582/en/Ant-Financial-Unveils-China%E2%80%99s-Credit-Scoring-System-Online (last visit No. 6, 2018)

[8] Chris Brummer & Yesha Yadav, *Fintech and the Innovation Trilemma*, GEO. L.J. 30 (2018, forthcoming).

[9] David Ingram, *Facebook says data leak hits 87 million users, widening privacy scandal*, Reuter, Apr. 5, 2018, available at https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM (last visited Nov. 6, 2018); Kevin McCoy, *Target to pay $18.5M for 2013 data breach that affected 41 million consumers*, USA TODAY, May 23, 2017, available at https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-

The issue of data protection gets even more difficult to manage when data is shared between financial institutions and nonfinancial firms. In recent years, many jurisdictions are implementing the so-called "open banking" policies to enable efficient customer data sharing between banks and payments service providers.[10] The European Union has been widely considered as a frontrunner in this regard because of its Payment Services Directive ("PSD 2") that came into force in January 2016.[11] Open banking policies generally require or encourage banks or account service providers to share their customers' data, upon the customer's demand, with third-party services providers through Applications Programming Interfaces ("APIs")[12] or other interfaces which allow safe and seamless transmission of data. Against this backdrop, data sharing between firms will take place more frequently and begs the question as to what safeguards can adequately protect consumer data across the firm and industry lines. Such second type of collaborations usually takes the form of data-sharing arrangments and will be analyzed later on.

Thirdly, rapid technological developments, and the increased market competition incentivize financial institutions to innovate and conduct trials on new technologies and operational models.[13] In most cases, these trials are conducted internally within the financial institution and referred to as Proof of Concept ("PoC"). A PoC, by its nature, is a *commercial experiment* and may involve other financial institutions and/or TPS as trial partners.[14] Although such commercial experiments will incur collaboration risks as previously mentioned, the scale and severity of the risk are generally controllable. What would involve greater risks are *regulatory experiments*, which usually take place when a firm's PoC goes beyond mere validation of technology or commercial viability, and when regulatory approval is required.

Regulatory experiments are typically conducted in the form of a pilot program or regulatory sandbox. Although much of the relevant literature considers the two

---

data-breach-affected-consumers/102063932/ (last visited Nov. 6, 2018)

[10] For example, the European, the UK, Australia, and Japan are among the jurisdictions where open banking polices are implemented through introducing legal mandates to the existing regulatory frameworks. Capgemini and BNP Paribas have recently conducted a Payment Open Banking Assessment and published their findings in the latest World Payments Report. The Report categories countries into pioneers, followers and conservatives based on how open banking is embraced in these countries. Brain Caplen, *Which Countries Lead in Open Banking?*, TheBanker, Oct. 19, 2018, available at https://www.thebanker.com/Editor-s-Blog/Which-countries-lead-in-open-banking (last visited Nov. 10, 2018)

[11] Ernst &Young, THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2) - WHAT YOU NEED TO KNOW (2018), available athttps://www.ey.com/Publication/vwLUAssets/Regulatory_agenda_updates_PSDII_Luxembourg/$FILE/Regulatory%20agenda%20updates_PSDII_Lux.pdf (last visited Jan. 4)

[12] As the U.S. Treasury noted, "API can be loosely described as a clearly specified program that links two or more systems and that enables a well-defined communication and data exchange between them in order to run applications and other software." U.S DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES – NONBANK FINANCIALS, FINTECH AND INNOVATION 26 (July 2018).

[13] For example, *see* Muyao Shen, *Major Banks, Regulators Trial 'Know Your Customer' App on R3's Corda*, COINDESK, June 29, 2018, available at https://www.coindesk.com/major-banks-regulators-trial-know-your-customer-app-on-r3s-corda (last visited Nov. 10, 2018); Pete Rizzo, *Bank of America Latest to Conduct Blockchain Trade Finance Trial*, COINDESK, Mar. 1, 2016, available at https://www.coindesk.com/bank-of-america-latest-to-develop-blockchain-trade-finance-trial (last visited Feb. 3, 2019)

[14] Commercial experiments involving trial partners are to be distinguished from industry consortia in which many financial institutions co-host repetitive rounds of experiments and to test applications or solutions that have a wider effect on the industry as a whole.

mechanisms conceptually similar, this paper analyses the nuanced differences between the two.[15] A pilot program is generally initiated by the financial regulator itself[16] and accompanied by a set of pre-determined regulatory requirements to give very clear guidance on how firms in the pilot program should carry out their business. A regulatory sandbox, on the other hand, is activated upon the application by the firm who wants to conduct a trial and then the regulator works out a flexible testing plan with the firm to ensure the trial proceed smoothly.[17] Pilot programs are often administered by the regulator to gradually open up a market, whereas regulatory sandboxes are mainly used by both the testing firm and the regulator to explore and redefine current regulatory parameters.

A regulatory experiment, be it a pilot or a sandbox, in effect gives the testing firm a restricted authorization or a limited license and allows the testing firm to engage real consumers over a certain period. Therefore regulatory experiments also pose risks to consumers and need to be properly overseen and regulated.[18] Some nonfinancial firms, especially start-ups, conduct regulatory experiments jointly with financial institutions either to get access to the financial institution's customer base [19] or to assure the regulator that they will (and have) the ability to comply with complex financial regulations.[20] Recently, some jurisdictions are even proposing the idea of cross-border trials which allow firms to "trial new ideas with consumers or other market participants in multiple jurisdictions working with the appropriate regulatory authorities."[21] In the foreseeable future, regulatory experiments that transcend both the country and industry

---

[15] For example, one literature treats "testing and piloting" as an alternative to regulatory sandboxes. Dirk A. Zetzsche et al., *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 FORDHAM J. CORP. & FIN. L., 31, 83-85 (2017).

[16] This means regulators, not the firms, decide which area should conduct a pilot.

[17] One of the main purposes of implementing regulatory sandbox is to allow the regulators to collaborate with the industry to facilitate innovation. Basel Committee on Banking Supervision, *supra* note 1, at 38 (noting that "[s]upervisors in some jurisdictions have put in place initiatives to improve interaction with innovative financial players that could facilitate innovative technologies and business models for financial services, for example innovation hubs, accelerators and regulatory sandboxes."); *See also* Douglas W. Arner et al., *Fintech, Regtech and the Reconceptualization of Financial Regulation*, 37 NW. J. INT'L. L. & BUS., 371, 383 (2017).

[18] A regulatory sandbox usually poses risks to consumers in two ways. First, risks present during the testing period when the testing firm fails to implement effective safeguards to protect consumers from unintended losses, data breach or cyber-attacks. Second, some firms may use the regulatory sandbox to legitimize their unauthorized schemes. Lev Bromberg, Andrew Godwin and Ian Ramsay, *Fintech Sandboxes: Achieving A Balance between Regulation and Innovation*, 28 J. BANKING & FIN. L. & PRAC. 314 (2017).

[19] FIN. CONDUCT AUTH., REGULATORY SANDBOX LESSONS LEARNED REPORT 17 (Oct. 2017) (summarizing the limitations of sandbox testing and finding that "[p]artnerships between large firms and start-ups in the sandbox have proven to be successful for both parties, particularly for giving the start-up access to a larger pool of existing customers to test with."); HONG KONG MONETARY AUTHORITY, FINTECH SUPERVISORY SANDBOX (FSS), available at https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml (observing "[b]anks and their partnering tech firms that use the FSS are able to gather real-life data and user feedback on their new fintech products or services more easily, so that they can make refinements to them as appropriate before the full launch. Hence, the FSS can facilitate banks and their partnering tech firms to rollout fintech initiatives earlier, at a lower cost and with better quality upon full product launch.")

[20] In fact, some jurisdictions' regulators even encourage start-ups or nonfinancial firms to cooperate with financial institutions to apply for, and conduct, sandbox testing. Taiwan and Hong Kong are the examples.

[21] ABU DAHBI GLOBAL MARKET ET AL., GLOBAL FINANCIAL INNOVATION NETWORK (GFIN) CONSULTATION DOCUMENT 11 (Aug. 2018), available at https://www.fca.org.uk/publication/consultation/gfin-consultation-document.pdf (last visited Nov. 6, 2018)

boundary will take place more frequently, which begs the question of how legal liability and regulatory responsibility can be adequately allocated among the firms which conduct trials together. Regulatory experiments can be treated as the third type of collaborations.

Finally, financial institutions also form industry consortia with both one another and nonfinancial innovators to develop new applications and explore new ways to minimize costs and risks.[22] Unlike the usual commercial experiments conducted within a financial institution, consortia serve as a co-working platform for many financial institutions to conduct repetitive rounds of experiments and to test the use and potential applications of certain burgeoning technology with the aim of solving an industry-wide pain point. In a 2017 survey on digital innovation in financial services, 72 percent of the 200 respondents (executives from large banks and investment firms) considered industry consortia to be vital to the development of solutions.[23]

Blockchain consortia present probably the most salient example. According to a recent International Financial Corporation report's summary, there are over 40 blockchain consortia in the world, and a majority of them comes from the financial services sector.[24] A blockchain consortium is essentially a semi-private blockchain with an expandable membership which allows participating members to create "compartmentalized trust relationships and to condition access to the network accordingly."[25] Firms create blockchain consortia to tackle technical or business problems facing them and to develop interoperable and modular platforms across multiple industries.[26] Nevertheless, so far, most projects launched by blockchain consortia remain in the experimentation stage, and many are arguably overhyped. By far the most successful blockchain consortium that has demonstrated its ability to solve problems on this scale is the JPMorgan-led Interbank Information Network (IIN).[27] The IIN enables participating members to transfer US currency across borders more efficiently and quickly and is said to be able to handle more than 300,000 transactions per day.[28] It has 123 banks as its members as of November 2018.[29]

Huge-membership consortia inevitably present governance issues as interests of members are necessarily divergent. Indeed, about 60% of the afore-mentioned survey respondents "believe that many consortia involve too many organizations to be effective."[30] Membership size does not necessarily lead to the ineffective function of a consortium, but it surely adds another layer of complexity into the governance of the

---

[22] Int'l Fin. Corp., *Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Markets*, EMCOMPASS NOTE 4 (Sept. 2018)

[23] SIMMONS &SIMMONS, HYPERFINANCE - ACCELERATING DIGITAL INNOVATION IN FINANCIAL SERVICES 20 (2017), available at https://www.finextra.com/finextra-downloads/newsdocs/simmonssimmons-hyperfinance-report-int.pdf (last visited Nov. 20, 2018); Noelle Acheson, *The Next Phase of the Blockchain Consortium Is Here*, CoinDesk, April 24, 2017, available at https://www.coindesk.com/next-phase-blockchain-consortium (last visited Nov. 20, 2018)

[24] Int'l Fin. Corp., *supra* note 22 (citing *Deloitte analysis and Gratzke, Peter, David Schatsky and Eric Piscini. 2017. "Banding Together for Blockchain - Does it Make Sense for Your Company to Join a Consortium?" August 16, 2017.*)

[25] *Id*.

[26] *Id*.

[27] Laura Noonan, *Banks Find A Use for Blockchain: Cross Border Payments*, FIN. TIMES, Nov. 12, 2018, available at https://www.ft.com/content/57b1064a-c1a5-11e8-84cd-9e601db069b8 (last visited Nov. 20, 2018)

[28] *Id*.

[29] JPMorgan, *Largest Number of Banks to Join J.P. Morgan Interbank Information Network*, available at https://www.jpmorgan.com/global/treasury-services/IIN (last visited Nov. 20, 2018)

[30] Simmons &Simmons, *supra* note 23, at 20.

already difficult-to-manage group of multiple stakeholders. This complexity begs the question of how to ensure effective interaction, decision-making, and risk management among consortium members.[31] These industry consortia make the fourth type of collaborations.

The preceding analysis suggests that the fintech-era collaborations take four broad forms: *Third-party service relationships*, *data-sharing arrangements*, *regulatory experiments*, and *industry consortia*. Each presents certain risks or governance issues to the consumers, the participating firms, and the financial market as a whole. These risks and governance issues are not necessarily foreign or novel to the regulators. Financial regulators have been dealing with (and perhaps are good at tackling) risks that may have a negative impact on the financial system and financial consumers, such as micro and macro-prudential risks. However, in the past, these risks mainly arise from operations of financial institutions or collaborations and interconnections among financial institutions. In the fintech era, a significant degree of risks was derived from collaborations between financial institutions and non-financial firms. These risks might subject financial institutions to operational failures, systemic data breach, or institutional insolvency, and introduces new challenges to financial regulators. As the Financial Stability Board ("FSB") pointed out in a recent report, "[r]Reliance by financial institutions on third-party data service providers … for core operations is currently estimated to be low. However, following the trend in other industries, some analysts predict that reliance will increase going forward. **If high reliance were to emerge, along with a high degree of concentration among service providers, then an operational failure, cyber incident, or insolvency could disrupt the activities of multiple financial institutions** [emphasis added]. Thus, while increased reliance on third-party providers specialising in cloud services may reduce operational risk at the individual firm level (idiosyncratic risk), **it could also pose new risks and challenges for the financial system as a whole, particularly if risks are not appropriately managed at the firm level, and if the complexities and interconnectedness of third parties and their usage continue to grow.** [emphasis added]"[32] In other words, fintech-era collaborations present risks which financial regulators might not be necessarily familiar with. These risks include data privacy risk, cyber risk as well as operational and competition risks arising from interactions between financial institutions and non-financial firms. Should the frequency and intensity of these collaborative activities increases, financial regulators will probably find themselves run short of proper regulatory expertise and tools to effectively address risks that arise. The most urgent challenge facing the regulators, therefore, goes deeper than understanding what these risks and issues are and lies in whether the regulators have the proper regulatory approach or toolkit at hand to help them *continuously* identify, evaluate and address the issues that arise as these fintech-era collaborations deepen further.

This paper argues that a novel regulatory approach is needed to ensure proper supervision of the risks that arise from the four forms of fintech-era collaboration.[33] At least three distinctive features of these fintech-era collaborations justify the need to address the issues with a novel regulatory approach.

---

[31] *See* Int'l Fin. Corp., *supra* note 22, at 5.

[32] FIN. STABILITY BD., *infra* note 49, at 2.

[33] Some countries have also noted the need to consider new regulatory approaches. *See e.g.*, U.S Dep't of the Treasury, *supra* note 12, at 13 (advocating that "[f]inancial regulators must consider new approaches to effectively promote innovation, including permitting meaningful experimentation by financial services firms to create innovative products, services, and processes.")

First, unlike in the past where a financial institution usually outsourced part of its activities or services to a third-party provider that was either a financial institution for custodial services[34] or a utility provider such as a telecommunication company providing broadband services, financial institutions today usually make arrangements with fintech firms or technology companies to outsource the storage and processing of customer data or even some of the financial institution's core operations. For example, Starling Bank in the UK used Amazon's AWS to build all of its infrastructures.[35] It is a typical example of a bank outsourcing its core operations to a cloud service provider. There are also some examples where financial institutions collaborate with technology firms to enable AI solutions.[36] As some commentators argued, existing regulatory framework "is geared to traditional architectures /legacy IT,"[37] and therefore casts doubts over whether the use of new technologies such as the cloud "can actually fit under an existing regulatory structure."[38] Generally speaking, these modern forms of outsourcing present regulatory challenges in three ways. First, the outsourced firm are not themselves regulated financial institutions, and therefore, financial regulators do not necessarily know what risks will evolve from the outsourcing arrangement and may lack proper tools to manage those risks. Second, these outsourced firms sometimes are much bigger than the outsourcing firms, and, therefore, it casts doubts over whether the outsourcing firm is able to effectively monitor the outsourcing relationships. Regulators may no longer rely solely on the outsourcing financial institution to manage the third-party risks that arise from the outsourcing arrangement. Third, these outsourcing activities usually involve sharing and processing of customer data and therefore begs the question of whether financial regulators own proper expertise and capacity to supervise potential data risks.

Second, these collaborations usually involve activities of not-yet-regulated fintech firms. Due to the lack of experiences regulating these firms, financial regulators know very little about risks that may arise from their actions and operations, not to mention risks from their collaborations with regulated financial institutions or other non-regulated firms. Even if these firms apply for certain regulatory relaxations and are allowed to operate under limited authorizations such as those provided by a regulatory experiment, the supervisory purview and existing regulatory system might still not

---

[34] For example, financial institutions have for decades outsourced custodial services to other financial firms such as State Street and BNY Mellon.

[35] Asha Barbaschow, *Starling Built A Bank from Scratch in the Cloud*, ZDNet, No. 28. 2018, available at https://www.zdnet.com/article/starling-built-a-bank-from-scratch-in-the-cloud/ (last visited July 2, 2019)

[36] For instance, Wells Fargo began piloting an AI-driven chatbot through the Facebook Messenger platform with their employees. This virtual assistant will communicate with users to provide account information and helps customers reset passwords. Kumba Sennaar, *AI in Banking – An Analysis of America's 7 Top Banks*, EMERJ, June 13, 2019, available at https://emerj.com/ai-sector-overviews/ai-in-banking-analysis/ (last visited July 2, 2019)

[37] INST. OF INT'L FIN., CLOUD COMPUTING IN THE FINANCIAL SECTORPART 2: BARRIERS TO ADOPTION 2 (OCT. 2018)

[38] *Id*. (Elaborating by using the example of cloud and explainingt that "[t]o some, cloud is simply a form of outsourcing, meaning that any imple-mentation by a bank or insurer must be subject to a set of standards that were historically developed and applied to other (non-digital) outsource providers. Some other regulators see cloud more as a utility, where the CSP role is like that of an electricity supplier or a telecommunications company. But there are also other views in the direction that cloud might be considered in the future (as more material applications, processes and data are migrated to cloud) as a critical infrastructure with oversight of CSPs. **These divergent views perhaps reflect the challenges of an existing framework that is geared to traditional architectures / legacy IT, and struggles to handle the type of scenarios that arise under new technologies like cloud** [emphasis added])

holistically address potential risks. Regulators, therefore, face the challenge of "*regulating as they learn*." Such a challenge is by no means new to the regulators but is probably made more difficult as the sheer amount of demand for market entry and limited authorizations by fintech firms have forced regulators to make quick and frequent decisions.

Third, these collaborative initiatives generally require a well-crafted governance regime among participating institutions to effectively allocate legal liability and compliance responsibility, and thus the efficacy of supervisory efforts lies heavily on how well regulators respond to, and collaborate with, that governance regime in play. These fintech-era collaborations not only call for a rethinking of the role played by regulators in supervising collaborations between financial institutions and nonfinancial fintech firms but also open the door for a new form of governance that might be achieved through novel regulatory approaches.

Part II of this paper provides an in-depth analysis of the regulatory implications for each of the fintech-era collaborations. Part III focuses on the recent developments of industry sandboxes and discusses how regulators can use them to help manage risks arising from fintech-era collaborations. It further argues that, with the proper use of supervisory technology (SupTech), an industry sandbox has the potential to be turned into a supervisory control box and to help develop a new paradigm of technology-enabled regulator-industry collaboration. Part IV proposes a tentative roadmap for future reforms. Part V concludes.

II. FINTECH-ERA COLLABORATIONS AND THEIR REGULATORY IMPLICATIONS

Each of the fintech-era collaborations subjects participating firms, and sometimes, financial consumers or the market as a whole, to certain risks. Regulators and the participating firms need to prepare safeguards to manage these risks. Section A to Section D present a risk analysis of each collaboration type and identify corresponding regulatory implications. Based on the identified regulatory implications, Section E then examines whether the current outsourcing regulatory regime under which fintech-era collaborations are governed is able to effectively address and respond to those implications. It then conducts a holistic and comparative review of the existing outsourcing regulations upon which worldwide financial regulators rely on regulating collaborations between firms. The review finds contemporary outsourcing regulation builds on dated, and now questionable, assumptions and fails to effectively respond to challenges arising from fintech-era collaborations and therefore argues that a novel regulatory approach is needed.

A. Third-Party Service Relationships

Third-party service relationships ("TPS relationship") generally take the form of outsourcing arrangments. Outsourcing arrangements broadly defined include any arrangements in which a service provider undertakes to provide a service for a financial institution, and such a service is normally performed by the financial institution itself.[39] TPS relationships and outsourcing arrangments can transcend geographical boundaries

[39] *See* MONETARY AUTH. OF SIN., GUIDELINE ON OUTSOURCING 7 (July 2016); H.K. MONETARY AUTH., SUPERVISORY POLICY MANUEL ON OUTSOURCING 2 (Dec. 2001).

and undertaken by overseas service providers. From a financial regulatory point of view, TPS relationships subject the outsourcing financial institution to operational, reputation and compliance risks that arise from the failure of the service provider or its inability to comply with regulatory requirements.[40] If many financial institutions outsource some function to a single service provider, it will also subject these institutions to concentration risks that may potentially destabilize the entire financial system.[41] Some even recognize the so-called "step-in risks," which will lead the outsourcing institution to feel obliged to bail out its service provider should things go south.[42] Step-in risks might not be very salient but are not unperceivable. For example, if a bank relied on its outsourced institution's technological solutions to carry out cross-border remittance services, such as using blockchain to replace traditional correspondent banking model, then if for some reason the outsourced institution encounters operational failures and is close to insolvency, the bank might well choose to bail out its outsourcing partner so as to closely review the problems and try maintaining continuity of the remittance service and the bank's reputation.

Contemporary financial regulation has long addressed risks introduced by TPS relationships or outsourcing arrangements. Typical safeguards include legal or regulatory requirements for the outsourcing institution to do the following: to conduct due diligence before engaging a service provider, to reach consensus over the outsourcing arrangement with the service provider in the form of outsourcing agreement or a concrete outsourcing policy, to have in place sound internal governance arrangements, and to get regulatory approval wherever necessary. The nature and scope of the TPS relationship decide the level of regulatory scrutiny adopted. Many jurisdictions, for example, distinguish between *critical* and *material* outsourcing activities and subject them to different sets of regulatory standards or requirements. The level of regulatory scrutiny might differ. However, essentially every jurisdiction provides that outsourcing arrangements do not relieve the outsourcing institution and its board and senior management of their obligation to comply with relevant regulations and ensure the service provider conducts the outsourced activities safely.[43]

The regulatory thinking behind the preceding designs seems to suggest that the regulators believe that the outsourcing institution *should and can* effectively supervise the service provider during the process of carrying out outsourced activities. Such presumptions might have held in the past but may not necessarily be sustainable in the fintech era. Technological or innovative solution providers today are often very big in their corporate size or asset level, and sometimes even outsize financial institutions. Cloud services providers, for example, are typically very large and include well-known brands such as Amazon, Microsoft, Google, Alibaba, and Tencent. Unlike the traditional Internet, email or data storage services, cloud services encompass "a range of IT services provided in various formats over the Internet."[44] A cloud service provider offers not only data storage solutions but also computing and data analytical services. In other words, the services and products cloud providers are selling are much

[40] Monetary Auth. of Sin., *Id.* at 1. For a list of the relevant risks, *see* BD. OF GOVERNORS OF THE FED. RESERVE SYS., GUIDANCE ON MANAGING OUTSOURCING RISK 1-2 (Dec. 2013).
[41] Bd. of Governors of the Fed. Reserve Sys., *Id.*
[42] EUR. BANKING AUTH., CONSULTATION PAPER - EBA DRAFT GUIDELINES ON OUTSOURCING ARRANGEMENTS 11 (June 2018).
[43] *See e.g.*, Bd. of Governors of the Fed. Reserve Sys., *supra* note 40, at 2; Monetary Auth. of Sin., *supra* note 39, at 1.
[44] FIN. CONDUCT AUTH., FG 16/5 GUIDANCE FOR FIRMS OUTSOURCING TO THE 'CLOUD' AND OTHER THIRD-PARTY IT SERVICES 2 (July 2018).

complicated, and banks are usually having difficulties in telling and pricing the differences in the service quality. Additionally, unlike traditional data storage or IT services for which banks have many vendors to choose from, banks only have minimal choices over cloud service providers, especially when it comes to the provision of large amount storages, high-speed computing, and cutting-edge machine learning technologies. Limited choice subjects banks to bargaining disadvantages when procuring cloud services. It is probably unrealistic to expect a city or community bank which outsources its information processing activities to Amazon to adequately supervise Amazon's cloud services platform and hold itself responsible for whatever loss incurred from Amazon's omissions or misconduct. The size of Amazon and the complexity of its cloud services and operations make smaller banks very difficult to employ any meaningful supervision.

Using the cloud can spare financial institutions from the burden of building and retaining large computing powers and thus gives them greater flexibility to allocate resources and enable innovation.[45] Cloud services generally involve the use of computing resources over the Internet and are scalable.[46] The range of cloud services includes private, public or hybrid cloud, as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).[47] A recent empirical study on the use of clouds by banks showing that banks indeed increasingly rely on cloud services. For instance, in December 2015, about 85% of Goldman Sachs' workloads operated in a cloud framework and TD Bank in Canada moved 98,000 employee email accounts to Microsoft's Office 365 in the same year.[48] Consulting firms, such as Gartner, predicts that "total global spending by financial institutions on public cloud services to grow from $37 billion in 2017 to $55 billion in 2020."[49] Generally speaking, large banks usually have their own data centers already and thus are more reluctant to use the cloud for either cost efficiency reason or data security concern. Whereas smaller banks or challenger banks may resort to cloud services due to limited IT budgets and with the aim to reduce entry costs and time to the market.[50]

As recognized by the UK's Financial Conduct Authority, "[c]loud customers may have less control of the supplier, for example, the degree to which they can tailor the service provided, and of the data, such as where data are stored."[51] The problem of having less control of the cloud service providers does not just occur after the outsourcing arrangement is made. During contract negotiations, financial institutions often find themselves enjoying less bargaining power, especially when dealing with big providers. As the empirical study uncovered, "universally so far (quotation marks omitted) negotiations have started from the provider's standard terms, although banks

---

[45] *See Id.*

[46] W Kuan Hon & Christopher Millard, *Use by Banks of Cloud Computing: An Empirical Study*, QUEEN MARY UNIVERSITY OF LONDON, SCHOOL OF LAW LEGAL STUDIES RESEARCH PAPER NO. 245, 6 (2016) (citing Hon, W.K., Millard, C. & Walden, I., 2013a. Negotiated Contracts for Cloud Services. In C. Millard, ed. Cloud Computing Law. Oxford, United Kingdom: OUP Oxford)

[47] Fin. Conduct Auth., *supra* note 45.

[48] Hon & Millard, *supra* note 46, at 11.

[49] FIN. STABILITY BD., FINTECH AND MARKET STRUCTURE IN FINANCIAL SERVICES: MARKET DEVELOPMENTS AND POTENTIAL FINANCIAL STABILITY IMPLICATIONS 7 (Feb 2019) (citing Fred Ng and Rajesh Kandaswamy, *Market Insight: Value-Based Cloud Opportunities in Financial Services*, GARTNER, April 2017.)

[50] Hon & Millard, *supra* note 46, at 11; *See also Id*. at 17 (noting that "cloud services may enable much smaller financial institutions access to far more sophisticated architecture and security features than they would be able to acquire on their own. Similar benefits may extend to start-ups, and to financial institutions in emerging market and developing economies.")

[51] Fin. Conduct Auth., *supra* note 45.

negotiate them "aggressively" to ensure clear risk management/allocation (required by FS regulation) as well other regulatory reasons. The challenge is meeting in the middle."[52] Evidence sometimes suggests that financial institutions may spend several years of heavy negotiation with some cloud service providers.[53]

Some bank also stated that "'the deal-breaker' has been the provider's unwillingness to negotiate language that the bank considers necessary to comply with its regulatory requirements."[54] Given the level of difficulty of negotiating with service providers, it is already unlikely for the outsourcing institution to try to embed effective controls of the TPS relationship in the outsourcing agreements, let alone to effectively exercise discipline over the service providers should things go wrong. In a situation under which many financial institutions want to outsource their respective functions or activities to the same service provider, a significant amount of capital will be wasted on contract negotiations and due diligence as many of these efforts might be duplicative and unnecessary even from a regulatory perspective.[55]

Another dimension makes the situation even more complicated. The increasing level of regulatory fragmentation, especially in the field of data protection regulation and banking regulation, has made financial institutions that have operations in multiple jurisdictions face greater compliance uncertainty and costs if they want to engage an overseas service provider.[56] Although many regulators have come to realize this issue, they have not yet fully developed a solution. Fragmentation presents in two dimensions. First, TPS relationships introduce not only financial regulatory issues but also data privacy and protection issues. For example, a growing number of jurisdictions have introduced various versions of data localization regulations.[57] Data localization requirements vary across jurisdictions. Some "restrictions apply to almost any data that has been collected or generated within the country, other requirements are more targeted and apply only to certain categories of data or to specific economic sectors."[58] Fragmentation may arise when financial institutions face different requirements under financial regulations and data protection regulations. Second, every jurisdiction has different sets of regulatory requirements for TPS relationships. Financial institutions might need to comply with different requirements when it comes to offshoring the storing and the processing of their data. To solve these two-dimensional regulatory fragmentations facing TPS relationships, financial regulators need to engage themselves actively in both cross-border cooperation with foreign financial regulators and cross-industry collaborations with regulators for other industries. In addition, fragmentation not only occurs in the formation of regulations but also in the

---

[52] Hon & Millard, *supra* note 46, at 33.
[53] *Id*.
[54] *Id*.
[55] Some jurisdictions, however, do take this into consideration and offer regulatory relaxations in this regard. *See e.g.*, OFFICE OF THE COMPTROLLER OF THE CURRENCY, DESCRIPTION: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULLETIN 2013-29 (June 2017).
[56] *See* Hon & Millard, *supra* note 46, at 38 (observing that "[e]ven if a bank can comply with the FCA's cloud guidance or other national guidance, compliance with regulatory requirements is obviously more challenging for those with multi-jurisdictional operations, within or outside the EU, as "They face different rules and they or their provider may not be able to comply with them all"").
[57] INST. OF INT'L FIN., DATA FLOWS ACROSS BORDERSOVERCOMING DATA LOCALIZATION RESTRICTIONS 1 (March 2019), available at https://www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf (last visted July 5th, 2019).
[58] *Id*.

enforcement of the regulation stage. It is also important for the regulators to pay greater attention to the enforcement of the TPS relationship governance.

Equally important is the level of regulators' knowledge about innovative technologies offered by the third party provider. Some findings have shown that regulators' knowledge about cloud service is limited.[59] As quoted by the empirical study, a regulator stated in an interview that "[r]egulators need to be prudent but many don't have the right knowledge to progress well with cloud; they don't know what to ask for from the bank or provider."[60] As the study further shows, some third party provider criticized financial regulators for lacking understanding of how cloud service works by stating that "[l]ots of rules or guidelines, even if written recently, don't understand how cloud works. This is very frustrating and impedes [bank] customers from using the world's most innovative platform. There is a disconnect."[61] Banks also raised similar complaints toward their regulators for the lack of sufficient understanding of cloud services.[62] Cloud computing is just one example of new technologies requiring regulators' prompt understanding. Decentralized financial technologies such as Distributed Ledger Technology ("DLT") have also been puzzling and challenging the regulators as to what risks would involve from the use of it and how does financial regulation should respond to it.[63] This probably explains why it takes years for many jurisdictions to decide whether and how to regulate activities such as Initial Coin Offerings or Security Token Offerings. Regulators will not rush into making decisions to allow or disallow certain activities involving the use of novel technologies until they can make good sense of how the technology works. The level of technological knowledge and literacy of different regulators also varies, and that further hinders effective coordination among global regulators.[64]

The preceding discussions suggest, at the least, the following regulatory implications: First, the presumption that the outsourcing institution can adequately supervise the third party provider seems dubious as today's third-party providers are usually large in size and complex in the provision of their service solutions. Requiring the outsourcing institution to take full responsibility for the risks introduced by the service provider does not necessarily mean those risks will be properly overseen and managed. Regulators need to be very practical to create a mechanism which enables financial institutions to better harness the benefits from TPS relationships and adequately exercise supervision in a manner that is workable and acceptable to the third party service providers.

Second, a fragmented regulatory system does not seem to be able to address TPS relationships and the risks that arise effectively. In order to deal with the two-dimensional regulatory fragmentations as abovementioned, financial regulators need to engage themselves actively in both cross-border cooperation and cross-industry collaboration.Regulators also need to find a way to enable deeper and effective collaboration in both *ex-ante regulation* and *ex-post enforcement* of the TPS relationship governance.

---

[59] *Id*. at 35.
[60] *Id*.
[61] Hon & Millard, *supra* note 46, at 35.
[62] *Id*.
[63] For the risks, benefits and regulatory issues of using decentralized financial technologies, *see generally* Fin. Stability Bd., DECENTRALISED FINANCIAL TECHNOLOGIES REPORT ON FINANCIAL STABILITY, REGULATORY AND GOVERNANCE IMPLICATIONS 6-10 (June 2019).
[64] It is said Monetary Authority of Singapore is much more sophisticated when it comes to regulating banks' use of clouds. Banking examiners in the US are also said to have been trained on cloud services and virtualization. *Id*. at 35-36.

Third, regulators' lack of understanding about new technologies and their usages somehow slows down financial institutions' engagements in TPS relationships, domestically or internationally. Regulators need to educate themselves and continue to keep themselves informed about new developments in technology and perhaps work out a way to effectively communicate and learn from the service providers.

B. Data-Sharing Arrangements

Many have widely regarded data as the modern form of money in the financial industry. Some commentators even observed that FinTech has gradually moved "from the digitization of money to embrace the monetization of data."[65] Due to the advancement in technological innovations, firms' ability to capture and use customer data has dramatically improved.[66] Technologies such as Internet-of-things, cloud computing, data analytics, and machine learning allow companies to collect a greater variety of customer data, and enhance their capability to store, manage, transfer and analyze these data.[67] Expanded use of customer data, such as sharing with other service providers, can not only help financial institutions design customized or targeted services and products to improve customer experience but also boost economic growth by bringing new consumers into the financial system as financial institutions will have greater information to determine whether and how to serve a previously excluded customer.[68]

Data sharing, in theory, could take a variety of forms. It could take place between institutions or between customers and institutions. The contents and scope of data to be shared could include transaction data, customer identity data, other customer-provided data, product data, and value-added data aggregated by the institution itself.[69]

Both financial and nonfinancial firms have the incentive to cooperate in order to understand their customers better and make a profit by serving their customers better. In addition to the technological and economic factors, regulatory actions also give momentum to data-sharing activities. With an aim to protect consumers' data and encourage the reasonable use of customer data to enable innovation, many jurisdictions have developed relevant legal and regulatory safeguards. These safeguards often come with supporting mechanisms such as the grant of legalized rights to the consumers to help them control their data and to establish critical infrastructures to allow data transmission and portability.[70] Salient examples include GDPR in Europe and open banking policies implemented by many jurisdictions such as the UK, Australia, Singapore, Hong Kong, and Canada.[71]

---

[65] Arner et al., *supra* note 17, at 402.

[66] WORLD ECON. FORUM, WHITE PAPER ON THE APPROPRIATE USE OF CUSTOMER DATA IN FINANCIAL SERVICES 6 (Sept. 2018).

[67] Business interaction among enterprises has been advancing data availability as well. PETER G. LEONARD, REGULATORY TRENDS AND EMERGING PRACTICES IN ACCESS TO CUSTOMER DATA, PORTABILITY AND DATA SHARING IN THE FINANCIAL SERVICES SECTOR 5 (December 3, 2017), available at SSRN: https://ssrn.com/abstract=3154275 (observing that "Data is more readily available because businesses interact with each other and with consumers through increasing flows of consumer data and because each businesses is increasingly algorithmically driven in its own operations.")

[68] *Id*. at 7

[69] THE AUSTRALIAN GOVERNMENT THE TREASURY, REVIEW INTO OPEN BANKING: GIVING CUSTOMERS CHOICE, CONVENIENCE AND CONFIDENCE 33-40 (Dec. 2017).

[70] *Id*. at 24-25.

[71] For each jurisdictions' approach and measures of open banking policies, *see* The Australian Government the Treasury, *supra* note 69; COMPETITION AND MKT. AUTH., MAKING BANKS WORK

As data-sharing arrangements taking place more frequently and at a larger scale, firms and the entire financial system are also facing greater risks. These risks include operational risk, cyber risk, data breach risk, reputational risk, and financial exclusion risk. Operational risk conceptually encompasses cyber and data risk as they both refer to situations where customers' data or privacy was breached due to cyber events or operational failures during the process of data-sharing. The reputational risk was incurred to financial institutions when negative events such as data breach occur. Financial exclusion risk generally means when data was used to profile customers and determine the costs of products or services, the algorithm may inadvertently generate biased conclusions that discriminate against groups which have less social or economic power and lead to financial exclusions of those groups.[72]

Some regulatory implications arise in light of the preceding discussion — first, the value and power of data-sharing manifest most when data is available in a form that allows easy aggregation and integration with other data sets.[73] Aggregated and integrated data has the potential to give rise to innovative financial products or services which better satisfy customers' needs. Standardized, portable and interoperable data formats can facilitate data aggregation and integration. However, interoperability and portability of data can only be achieved through regulatory coercion or facilitation otherwise industry players usually lack coordinated incentive to push for a single standard. The good news is that regulators also have the incentive to enable data standardization, interoperability and portability. In the age of Fintech, data serves as not only an important competitive edge for the industry players to better serve their customers but also a key foundation for the regulators to enable adequate regulation and effective supervision. However, many regulators find themselves having difficulty in collecting data on Fintech credit.[74] According to an FSB survey among 23 jurisdictions conducted in August-October 2018, the top three practical challenges in collecting data on FinTech Credit were "(i) the lack of a clear definition for Fintech credit; (ii) FinTech credit activities are not currently being included in jurisdictions' supervisory reporting; and (iii) market data not being reliable."[75] These challenges can be largely resolved through a refined supervisory reporting rule, standardized data format and reliable channels for data collecting and reporting. All of the above calls for the regulators to enable infrastructure and regulatory architecture that safely allow interoperability and portability of data. Such an enabling infrastructure would require a machine-readable standardized data requirement imposed by the regulator. These requirements will be in the form of regulatory rules and technical standards and sometimes also call for the creation of a data standard body to facilitate data creation.

HARDER FOR YOU (Aug. 2016); Heike Mai, PSD 2, *Open Banking and the Value of Personal Data*, Deutsche Bank Research EU Monitor, June 28, 2018; H.K. MONETARY AUTH., OPEN API FRAMEWORK FOR THE HONG KONG BANKING SECTOR (July 2018).

[72] Robin Nunn, *Discrimination and Algorithms in Financial Services: Unintended Consequences of AI*, PAYMENTSLAWADVISOR, available at https://www.paymentlawadvisor.com/2018/03/06/discrimination-and-algorithms-in-financial-services-unintended-consequences-of-ai/ (last visited Dec. 18, 2018).

[73] Leonard, *supra* note 67, at 5.

[74] According to the FSB, FinTech credit can be categorised into: "(i) entities not controlled by a financial intermediary whose business model is to facilitate directly or indirectly the granting of loans to borrowers through capital raised from investors; (ii) entities that perform the business model noted in (i) but which are controlled by a financial intermediary (eg "notarised" matching platforms); and (iii) entities that are not part of a banking or financial group, but with a more articulated business model, which includes activities usually performed by financial intermediaries (eg "balance sheet lenders")." FIN. STABILITY BD., GLOBAL MONITORING REPORT ON NON-BANK FINANCIAL INTERMEDIATION 2018 69 (February 2019).

[75] *Id.* at 70.

Second, data sharing activities subjects data owners and customers to increasing cyber and privacy risks and begs the question of how liability among all parties in a sharing arrangement should be reasonably allocated. The design of liability sharing will affect institutions' and consumers' willingness to share data and the level of supervisory resources input. There are several perceivable approaches to the design of liability sharing. First of all, data transmitting and receiving institution can resolve liability sharing issues by simply resorting to the concerning jurisdiction' civil law principles or statutory rules. This approach will subject liability sharing to a case by case exercise. Second, the regulators can impose a default rule which requires regulated financial institutions, when acting as the data transmitting institution, to be held accountable for the consumers (data subjects) and shoulder the liability first. The financial institution then can go to its data-sharing counterparts for indemnification. This approach will subject the data transmitting financial institution and the data receiving nonfinancial institution to typical outsourcing regulatory principles. The third approach would be to encourage the industry to develop consensus over liability sharing rules and form a self-regulatory code to enforce the consensus. This approach should engage all the stakeholders and ensure fair and inclusive participation of nonfinancial institutions. Locating an ideal liability sharing regime is of course not an easy task and goes beyond the scope of this paper, but if a proper liability sharing regime exists, regulators can concentrate their limited supervisory resources on areas where public enforcement is needed to ensure compliance with the liability sharing rules.

C. Regulatory Experiments

Regulatory experiments, such as regulatory sandbox regimes, have been implemented by many jurisdictions around the world.[76] Some of them are only open for non-financial institutions, whereas the majority allows both financial institutions and nonfinancial firms to conduct tests in the sandbox.[77] Regulatory experiments allow the regulators to closely observe the testing firms and identify risks that may arise from the business or operation in the trial. Experiments also create a friendly environment for entrepreneurs to freely discuss their concern with the regulator and thus enhances communication between the two.[78] Regulators can then, based on lessons learned from the sandbox experiment, navigate toward an ideal regulatory regime for the tested businesses once these businesses are launched officially in the market. In other words, regulatory experiments function as a data-collecting mechanism for the regulators to collect more data to carry out data-driven and empirical based regulatory measures.

Despite the fact that regulatory experiments can serve as an important source for regulatory and supervisory data, "regulators often note having few official data sources to monitor the sector, in part because entities fall outside the regulatory perimeter or are not registered to participate in sandboxes, innovation hubs, or accelerators."[79] Some fintech firms are not regulated as financial institutions and therefore are not necessarily obliged to report data to financial supervisors. For example, many crypto-

[76] For a summary of regulatory sandboxes in operation across the globe, *see* Zetzsche et al., *supra* note 15, at 64-68.

[77] For example, United Kingdom, Singapore, Malaysia, the Netherlands and Taiwan do not limit the sandbox's scope to financial institutions. Australia, however, limits the scope to the experiments of services providing advice in relation to eligible products and dealing in eligible products. Likewise, Hong Kong's sandbox regime only allows banks to conduct testing.

[78] Zetzsche et al., *supra* note 15, at 78.

[79] Fin. Stability Bd., *supra* note 1, at 59.

assets trading platforms, though *de facto* facilitating the purchase and selling of securities, have not been regulated as traditional stock exchanges or alternative trading systems due to the lack of clear mandates or doubt-free interpretations of the existing laws.[80] These platforms may be required to comply with reporting obligations under Anti-Money Laundering laws, but generally, are not required to report data to financial regulators as typical stock exchanges do.[81] If these unregulated institutions do not choose to conduct experiments in the sandbox or join other regulatory initiatives, regulators will lack channels for accessing data relating to their operations. Therefore, how to make regulatory sandbox regime more friendly and accessible for nonfinancial firms and fintech companies should be on top of the regulators' priorities. A more accessible sandbox regime would enable greater data availability and further inform regulators' decision-making.

A viable way to enhance data collection during the sandbox experiment would be to encourage firms to conduct tests together. The benefits of this approach are twofold: first, regulators will be able to collect some data on firms outside the regulatory parameter as these firms are now testing with regulated firms and need to comply with requirements and obligations set forth by the regulator. These data might include information about whether the non-regulated testing firm has qualified personnel and adequate IT system and capacity to carry out financial services, and information about whether the firm's operational and governance structure can readily respond to risks that arise during the firm's engagement in the experiment. The second benefit lies in the non-regulated testing firm's ability to legally access the regulated testing firm's customer data. This makes particular sense for smaller nonfinancial firms as it is generally very difficult for them to go and get data directly from the financial institution due to legal and regulatory constraints and thus testing in the sandbox with financial institutions presents a golden opportunity to make data sharing possible.

Although entities conducting sandbox experiments are not fully regulated, these experiments carried are out in a controlled environment, and thus the testing firm and the regulator can still manage risks through pre-agreed safeguard arrangements. Such arrangements may include a ceiling on the monetary amount and the number of consumers involved, a modified set of conduct and disclosure obligations, membership requirement of an external dispute resolution scheme, and adequate compensation arrangements when consumers suffer unanticipated losses during the testing.

In Taiwan, testing entities in the sandbox are required to implement a risk management regime based on the professional level of consumers and possible risks associated with the testing, in particular, cyber risk, money laundering risk, and data privacy risk.[82] The testing firm needs to put in place an appropriate compensation mechanism which includes entering into a trust agreement with the bank or obtaining the bank guarantee by which the bank undertakes the performance obligation of the

---

[80] For a recent, global survey of regulatory developments on crypto-assets, *see* FIN. STABILITY BD., CRYPTO-ASSETS REGULATORS DIRECTORY (April 2019).

[81] For example, in the US, firms that provide services related to virtual currencies can be classified as money transmitters and are sbject to Money Service Business registration, reporting, and recordkeeping requirements. . FinCEN in 2013 issued a guidance on Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, which differentiates regulatory treatment between "user", "exchanger" and "administrator" of virtual currencies. *See* FIN. CRIMES ENFORCEMENT NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (March 2013), *available at* https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (last visited July 7, 2019).

[82] *See* Taiwan's Financial Technology Development and Innovative Experimentation Act (2018).

testing firm to its consumers.[83] The relevant regulation also requires the testing firm to submit progress reports on a regular basis and contingency reports whenever there occurs a material event as defined by the regulation.[84] The regulator can also revoke the approval for the testing when the testing involves a situation that is materially adverse to the financial market or the interests of consumers.[85] All these protective measures and safeguards suggest that even there might still be consumer risks or operational risks during the sandbox experiment, it is hard to image these risks will turn into any systemic events. As the UK experience shows, according to the FCA's first-year experience, all sandbox tests were able to comply with their required standard safeguards.[86]

In cases where financial institutions and nonfinancial firms conduct a regulatory experiment together, the biggest risks may lie in the failure to protect consumers' data and the operational failure to carry out the cooperation smoothly. The mitigation of these risks generally requires a well-crafted governance arrangement between the cooperating firms and an effective supervisory system to ensure compliance of the governance arrangement. The former can be realized through proper contractual designs but the latter needs to involve regulatory oversight. Financial regulators generally do not own the expertise to supervise nonfinancial institutions. Therefore it is likely in a cooperative experiment most compliance burden may still lie with the financial firm. Such a result may reduce financial institutions' willingness to conduct regulatory experiments with start-ups, technology companies or other nonfinancial firms as that will increase the financial firm's compliance cost and reputational risks. If this is the case, then the regulator will not be able to maximize its data collection capacity and thus undermines the usefulness of regulatory experiments.

Regulatory implications that arise from the preceding discussion include the following: First, regulators may consider creating an environment that is easy and accessible for financial institutions and nonfinancial firms to conduct experiments collaboratively. Such an environment may include a clear set of regulatory requirements or guidance to instruct how the two types of institutions can collaborate. One example, to which regulators can refer, is the *Guide on Supporting Fintechs in engaging with Financial Institutions* proposed by the British Standards Institution, which aims "to lay out guidance for fintechs that will help them understand, prepare for and more easily navigate the path to forming successful engagement with large financial institutions."[87] Such guidance allows firms to conduct experiments quickly based on mutually-understood standards without spending too much effort and cost to work out practical terms and details to govern the cooperative relationship.

Second, regulators can use regulatory experiments as a vehicle to learn and rethink how to effectively share regulatory obligations and compliance burdens between financial institutions and their nonfinancial counterparts when these institutions are in a *facing-consumers -together* relationship. The current regulatory thinking seems to place all the compliance burdens onto the financial institution, but this would dramatically reduce financial institutions' willingness to cooperate, especially when it

[83] Article 13 of Taiwan's Regulations Governing Financial Technology Innovative Experimentation (2018).
[84] *Id*. at Article 20 and 21.
[85] Article 15 of Taiwan's Financial Technology Development and Innovative Experimentation Act (2018).
[86] Fin. Conduct Auth., *supra* note 19, at 7.
[87] THE BRITISH STANDARDS INST., PAS201: 2018 SUPPORTING FINTECHS IN ENGAGING WITH FINANCIAL INSTITUTIONS – GUIDE (July 2018), at Introduction.

comes to co-designing a product, sharing customers' data, co-managing market channels and coordinating operational resources. If this becomes the case, then the potential of fintech may only be realized in silos and within the traditional industry boundaries. In the absence of sufficient empirical commercial and industry data, regulators will be reluctant to open up the financial services market and may eventually fail the efforts to promote financial inclusion.

D. Industry Consortia

With the development of cutting-edge technologies, businesses have a greater need to understand these technologies' potential usages, and realizing these usages in real-life scenarios. Nevertheless, exploring and testing new technologies usually present significant risks to the testing firm and involve costs that may never be compensated if the technology proves to be useless or unwelcomed by the market. Firms, therefore, often form consortia together to conduct technological tests, locate common commercial solutions and share the costs and risks that arise. Industry consortia generally mean a group, platform or a joint venture which includes several different firms as members and aims to pursue common goals. Industry consortia take a variety of forms such as R&D collaborations and cooperative utilities as well.[88]

The formation of a consortium made particular sense when the collaborative solutions brought up by the consortium can benefit the entire industry and create an ecosystem with network-effects. The creation of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) by the worldwide financial industry members present probably the most salient and successful case. In 1973, 239 banks from 15 countries established the SWIFT, a cooperative utility, to communicate about cross-border payments effectively, a common problem facing all the founding members.[89] Recent examples include a global trade finance platform, collaboratively developed by a consortium of five banks, called Batavia which builds on the IBM platform,[90] and a joint-venture company created by the five biggest banks in the US called TruSight, to streamline the work of vetting third-party service providers and partners.[91]

The benefits of forming industry consortium in the era of fintech are numerous. First, reducing duplications among member firms' R&D investments. The commercial use of many innovative technologies such as machine learning and distributed ledger requires significant R&D investments and resource input at the PoC stage. These investments are a significant burden for individual firms and might never pay off. Also, forming a consortium can reduce unnecessary investments by individual firms and concentrate firms' limited R&D capacity to areas collaborative efforts cannot offer value-added.[92]

Second, the use of novel fintech technologies generally requires scalability. Scalability becomes a greater challenge in developing fintech solutions as achieving it

---

[88] R&D collaboration is widely adopted in the US, especially during 1990s. Many collaborative R&D projects were launched in industries such as pharmaceuticals, petroleum, and weaponry. *See* David C. Mowery, *Collaborative R&D: How Effective Is It?*, 15 ISSUES IN SCI. & TECH. 37-44 (1998).

[89] https://www.swift.com/about-us/history (last visited Dec. 23, 2018)

[90] Fabio Keller, *Blockchain-Based Batavia Platform Set to Rewire Global Trade Finance*, Apr. 19, 2018, available at https://www.ibm.com/blogs/blockchain/2018/04/blockchain-based-batavia-platform-set-to-rewire-global-trade-finance/ (last visited Dec. 23, 2018)

[91] Dan Freed, *U.S. Financial Giants Create Consortium to Vet Third Party Suppliers*, Reuter, Nov. 14, 2017, available at https://www.reuters.com/article/us-usa-banks-vendors/u-s-financial-giants-create-consortium-to-vet-third-party-suppliers-idUSKBN1DE1TV (last visited Dec. 23, 2018)

[92] *See* Mowery, *supra* note 88, at 39.

often requires cross-industry collaboration. Testing in a silo by individual firms will not help achieve scalability unless the solution came up by the testing firm becomes widely acceptable by other industry members or even stakeholders that involve from different industries. Forming a consortium will speed up adoption of these technologies for all the participating members as they can enjoy knowledge spillover and learn from collective experiences.

Third, consortia may help create an "industry-wide vision of future directions for technological innovation," which might facilitate the formation of industry best practices in promoting the industry's collective interests and protecting consumers' benefits.

The use of consortia also brings risks and problems. First, piloting new technologies always introduces failures and incurs risks to not only the participating consortium members but also end-consumers. Members in a consortium are subjected to liability risks and costs of assessments necessary to provide a clear view of the liability risk as it is generally not very clear how legal liabilities will be allocated among the members, let alone in the context of international consortia where the determination of applicable laws always presents difficulties.[93] Consortia with huge-membership present greater governance issue as interests of members are necessarily divergent and difficult to manage. The achievement of effective interaction, efficient decision-making, and adequate risk management among consortium members becomes the most important objective of today's fintech consortia.

Second, the formation of consortia sometimes creates an unrooted vision of the future direction for the market or false sense of comfort among members, especially when the technologies in the trial are relatively immature.[94] Frequent formations of consortia may also create and further hype in certain technologies and eventually lead to industry-wide waste of resources. These false "industry consensuses" engender misguided policy-making and the allocation of regulatory resources and subject financial markets to the suboptimal situation.

Third, the fear of missing out may incentivize financial services providers to quickly and thoughtlessly join existing consortia or form their own consortia. Some initiatives, therefore, might lack well-defined objectives and well-thought-through collaborative arrangements and eventually lead to duplication of participating members' investments in R&D spending and human resources.

Last but not least, when an industry consortium becomes very large and popular, the exclusion or refusal of membership to the consortium usually introduce anti-competition concern. Indeed, as the OECD highlights recently in its issue paper, a blockchain consortium, if its access "is controlled jointly by existing members of the consortia (known as gating), access might become an essential input to compete in the market. Refusal to access the blockchain might be used to exclude maverick firms or new entrants." [95]

The preceding discussion holds the following regulatory implications. First, regulators may consider providing clear guidance to help industry members design the governance structure and liability framework in a consortium. Such guidance may include regulatory coordination efforts across jurisdictions to increase legal and

---

[93] Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, EUROPEAN BANKING INSTITUTE WORKING PAPER SERIES 14, 40 (Aug. 2017), available at SSRN: https://ssrn.com/abstract=3018214 or http://dx.doi.org/10.2139/ssrn.3018214

[94] Mowery, *supra* note 88, at 41.

[95] THE ORG. FOR ECON. CO-OPERATION AND DEV., BLOCKCHAIN TECHNOLOGY AND COMPETITION POLICY -ISSUES PAPER BY THE SECRETARIAT 7 (June 2018).

regulatory certainty among consortia members when negative events occur.

Second, industry collaboration in a consortium where regulatory participation is absent might be counterproductive. Regulators should consider whether to have a role in the operation of industry consortia in order to timely identify and channel misplaced industry vision and misguided best practices. This early participation on the side of the regulator is not equivalent to regulatory intervention. Unlike a gatekeeper, regulators can play the role of a coach to observe the actions and behaviors of the members in the consortium and stand ready to provide guidance in a dynamic manner.

Third, in a consortium where membership is opened to financial institutions and nonfinancial firms, financial regulators will need to collaborate with regulators in other industries. Such cross-industry regulatory coordination become pressing as technologies explored in the consortium are usually not yet mature, but its member institutions are generally pioneering leaders in their respective industries. The failure of these leaders will present negative signals to the market and bring public doubts to the respective regulator's ability.

E. The Need for a Novel Regulatory Approach

The categorization of the four types of fintech-era collaborations does not aim to provide an authoritative taxonomy. It mainly serves as a heuristic device, and therefore the four types of collaborations are not completely discrete but sometimes overlap. For example, in cases where banks engage with a TPS to conduct sandbox testing, the third-party service relationship will still govern the rule of liability allocation between the two institutions. Moreover, firms may subject themselves to more than one type of collaboration at the same time. For example, a bank may well share its customer data with payment service providers during a sandbox experiment. This scenario will subject the bank and the payments service provider to a third-party relationship which involves data-sharing arrangement and constraints imposed by the regulatory experiment.

Nevertheless, the categorization remains valuable as it provides a clear analytical framework to identify relevant regulatory implications and help regulators achieve greater regulatory and supervisory effectiveness. Table 1 summarizes the four collaborations and their relevant implications for the regulators as analyzed in Section A to D of this Part.

Table 1: Fintech-era Collaborations and Regulatory Implications

Collaboration Types	Regulators should or can
Third-Party Service Relationships	● Enable financial institutions to better harness the benefits from TPS relationships and adequately supervise in a manner that is workable and acceptable to the TPSs ● Enable deeper and effective collaboration in both *ex-ante* regulation and *ex-post* enforcement of TPS relationship governance ● Educate themselves and continuously keep themselves informed about the new developments in technology and work out a way to communicate and learn from the service providers
Data-Sharing Arrangements	● Enable an infrastructure and regulatory architecture that allows interoperability of data portability in a safe manner

	● Facilitate the creation of an adequate liability sharing regime
Regulatory Experiments	● Create an environment that is accessible for financial institutions and nonfinancial firms to conduct experiments collaboratively. ● Use regulatory experiments as a venue to learn and rethink how to effectively share regulatory obligations and compliance burdens between financial institutions and their nonfinancial counterparts when they are in a facing-consumers-together relationship
Industry Consortia	● Provide clear guidance to help industry members design the governance structure and liability framework for consortia. ● Consider playing a role in the operation of industry consortia to timely identify and channel misplaced industry vision and misguided best practices. ● Collaborate with regulators in other industries

The summary above suggests that an ideal system for regulating fintech-era collaborations should have the following characteristics or elements. First, the regulatory system should enhance financial regulators' capability and capacity to learn new technologies, collect data, and collaborate with regulators in other industries. Second, the regulatory system should allow the regulators to be in constant and close dialogue with the industry so as to facilitate the creation of ideal governance structure and liability framework among different stakeholders in fintech-driven collaborative initiatives. Third, the regulatory system should enable an information infrastructure and regulatory architecture that allows data interoperability and portability in a safe manner. Fourth, the regulatory system should help regulators continuously reflect regulatory parameters and explore adequate ways to regulate fintech collaborations and nonfinancial institutions. Below presents an analysis of the current regulatory regime and argues, using regulatory implications learned from the preceding discussions, that a novel regulatory approach is needed to balance the regulation and promotion of fintech-era collaborations.

The existing regulatory regime, across jurisdictions, relies heavily on so-called "outsourcing regulation" to oversee and manage risks that arise from these collaboration activities. These outsourcing regulations manifest in various forms such as guidance[96], regulation[97], and supervisory manual.[98] The author conducted a comparative study of the outsourcing regulations in the US, the UK, the EU, Singapore,

[96] Examples include Bd. of Governors of the Fed. Reserve Sys., *supra* note 40; OFFICE OF THE COMPTROLLER OF THE CURRENCY, DESCRIPTION: RISK MANAGEMENT GUIDANCE BULLETIN 2013-29 (Oct. 2013); FED. DEPOSIT INS. CORP., GUIDANCE FOR MANAGING THIRD-PARTY RISKS (June 2008), available at https://www.fdic.gov/news/news/financial/2008/fil08044a.html (last visited Jan. 5, 2019); Monetary Auth. of Sin., *supra* note 39; Eur. Banking Auth., *supra* note 42.

[97] For example, in Taiwan, outsourcing arrangements by banks are regulated by the Financial Supervisory Commission under the Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operation.

[98] These are typically booklets or manuals prepared for the financial supervisors to help them conduct examinations. Regulated financial institutions can also use these booklets or manuals to closely observe supervisory requirements. Examples include the Supervision of Technology Service Providers booklet of the FFIEC Information Technology Examination Handbook, and HKMA Supervisory Policy Manual on Outsourcing.

and Hong Kong in order to understand the common characteristics of these regulations. The author picked these jurisdictions because these places host the world's most attractive FinTech ecosystems[99] , and their outsourcing regulatory materials are readily accessible in English. The fact that these jurisdictions have active and booming fintech activities would theoretically increase financial institutions' demand to collaborate with fintech firms and therefore the scope and requirements of outsourcing regulations will have significant impacts on fintech collaboration activities. An understanding of these jurisdictions' outsourcing regulations will also inform this paper's discussion. The comparative study found the following common characteristics of contemporary outsourcing regulation:

1. The scope of the definition of "outsourcing," "outsourcing arrangement" or "third party relationship" is generally very broad so as to encompass any arrangement, by contract or otherwise, under which another entity undertakes to provide a service to a regulated financial institution. Many jurisdictions specify that the service undertaken by a third party needs to be a service that was previously carried out or may currently (or potentially) be performed by the regulated financial institution.[100] Some jurisdictions also specify that only "ongoing" outsourcing relationship will be regulated.[101]
2. Outsourcing is generally prohibited if the arrangement will result in compromising or weakening of the outsourcing institution's internal control systems or business conduct[102], or if the service provider is located at jurisdictions where access to information by the outsourcing institution is impeded or impossible.[103]
3. Usually, the regulation does not require the outsourcing institution to obtain prior regulatory approval unless the arrangement is considered as material or critical, or the outsourced function is performed in a foreign jurisdiction.[104]
4. The outsourcing regulation typically requires the outsourcing institution to have in place a risk management framework (including policies and procedures) "that [is] commensurate with the level of risk and complexity of its third-party relationships."[105] Such a risk management framework usually needs to cover risks in different stages of the entire life cycle for the third-party relationship including *third-party selection and due diligence*,

[99] There are various ranking systems for world's fintech ecosystems, the author chose the one published by Thomson Reuters. The ranking was conducted by the Institute for Financial Services Zug (IFZ) of the Lucerne University of Applied Sciences which uses factors associated with driving entrepreneurship and innovation and indicators related to financial technologies. According to the ranking, Singapore ranked Top 1, London (UK) ranked the 4th, Hong Kong ranked the 10th. Among the top 10 cities, five (Zurich, Geneva, Amsterdam, London, Amsterdam and Stockholm) located in the EU and two (New York City and San Francisco) located in the US. *2018 IFZ Global FinTech Rankings*, Thomson Reuters Labs, https://innovation.thomsonreuters.com/en/labs/portfolio/global-fintech-rankings.html#/ (last visited June 26, 2019).

[100] H. K. Monetary Auth., *supra* note 39, at 2; Monetary Auth. of Sin., *supra* note 39, at 7; Eur. Banking Auth., *supra* note 42, at 18.

[101] Monetary Auth. of Sin., *Id*;

[102] H. K. Monetary Auth., *supra* note 39, at 3.

[103] Monetary Auth. of Sin., *supra* note 39, at 24.

[104] It is noted that even in the case of material outsourcing or overseas outsourcing, some regulators such as the Hong Kong Monetary Authority and Monetary Authority of Singapore do not seem to require prior approvals.

[105] Office of the Comptroller of the Currency, *supra* note 96, at 2.

risk assessment of the outsourcing arrangement, *contract negotiation*, *ongoing monitoring*, and *contingency planning*.[106] Regulatory requirements for risk management might become more rigorous if the outsourcing arrangement is considered as material or critical outsourcing.

5. Material or critical activities basically include significant functions (e.g., payments, clearing and settlements in the case of banks), significant shared services, or other activities that could cause the outsourcing institution to face significant risk (e.g., have significant negative impact on customers or the institution's operations) if the service provider fails to meet expectations.[107]
6. The regulation typically requires the outsourcing institution to be responsible for overseeing the service provider and report to the regulator.[108] Many jurisdictions also require the outsourcing institution (and its board and senior management) to retain full responsibility and accountability for discharging the institutions' regulatory responsibilities.[109] For example, the regulation often requires the outsourcing institution to ensure the protection of confidentiality and security of customer information during the outsourcing period.
7. The outsourcing institution's failure to have an effective third-party risk management framework may be considered an unsafe and unsound banking practice and introduce serious regulatory consequences.[110]
8. The outsourcing institution generally manages the third party risk and potential liability through its outsourcing agreement with the service provider. The agreement usually establishes the outsourcing institution's right to audit and monitor performance, and even conduct an inspection. These may include provisions for independent internal or external audits of the service provider and the provider's relevant sub-contractors.[111]
9. The regulation normally enables mechanisms to allow the regulator of the outsourcing institution to exercise the contractual rights of the institution so as to access and even examine the service provider and its sub-contractors.[112] Such an audit right generally allows the regulator to obtain documents, information, and records of the institution "stored at or processed by the service provider and its sub-contractors."[113]

To sum up, the central rationale underlying the contemporary outsourcing regulatory regime is that outsourcing institutions can and should effectively supervise the service provider while they carry out their duties required by the outsourced

[106] Office of the Comptroller of the Currency, *Id*. at 2-8; H. K. Monetary Authority, *supra* note 39, at 3-6; Monetary Auth. of Sin., *supra* note 39, at 8-21; Bd. of Governors of the Fed. Reserve Sys., *supra* note 40, at 2.
[107] Office of the Comptroller of the Currency, *supra* note 96, at 2.
[108] For example, Hong Kong Monetary Authority requires that authorized institutions should ensure that they have effective procedures for monitoring the performance of the service provider and the risks. The control procedures should also be regularly reviewed by the internal audit. H. K. Monetary Authority, *supra* note 39, at 7.
[109] Bd. of Governors of the Fed. Reserve Sys., *supra* note 40, at 1-2; Fin. Conduct Auth., *supra* note 45, at 4-5 (2018).
[110] Office of the Comptroller of the Currency, *supra* note 96, at 9.
[111] Office of the Comptroller of the Currency, *supra* note 96, at 5.
[112] Monetary Auth. of Sin., *supra* note 39, at 22.
[113] *Id*.

activities. Regulators supervise the outsourcing financial institution and hold it accountable for ensuring its relationship with the service provider remains safe and sound during the life cycle of the TPS relationship. The outsourcing institution generally needs to include regulator-required contractual terms in the outsourcing agreement in order to fulfill its regulatory responsibilities. These contractual terms give comfort to regulators when overseeing financial institutions' relationship with a third-party service provider and regulators will only intervene when their examination mission requires and when they feel the outsourcing institution does not perform its job well. This situation is evident as a recent Basel Committee on Banking Supervision report has demonstrated that "the majority of supervisors responded that they supervise third-party service providers only under limited circumstances and had no programme in place."[114]

Such rationale seems to build upon certain assumptions: First, service providers are typically not directly regulated or supervised by the financial regulators so regulators can only exercise authority over the regulated outsourcing institution.[115] Second, the outsourcing institution enjoys greater bargaining power when negotiating with the service provider. Therefore, the outsourcing institution should either be able to allow the service provider to impose all the regulator-required terms or walk away and find alternative solutions. Third, most outsourcing arrangements take place domestically. Fourth, each financial institution's outsourcing relationship should be managed separately although many financial institutions can collaborate to meet common responsibilities for managing a relationship with a common service provider.[116]

These assumptions might not necessarily hold in the era of fintech. As the paper has analyzed, fintech developments incentivize and enable financial institutions to more actively and frequently collaborate with their counterparts, small fintech start-ups, and giant technology services providers, either domestically or internationally, in scenarios including commercial experiments, regulatory trials, and industry-standards-advocating consortia.[117]

The existing outsourcing regulation might disincentivize financial institutions to engage in fintech-era collaborations as their oversight costs for outsourcing relationships may increase as forms of collaboration become diverse and complex with technological and market evolution. For example, as the Institute of International Finance ("IIF") pointed out, regulations have become barriers to financial institutions' adoption of cloud computing deployments.[118] The IIF paper argues that "[a] risk-based approach is important for [Financial institutions]. By basing their controls and compliance on an analysis of the risk posed by any activity or process, they can design mitigation strategies tailored to the specific risk and which allow the flexibility needed to account for the possible decrease or increase in risk posed by the activity."[119]

---

[114] Basel Comm. on Banking Supervision, *supra* note 1 , at 36-37.

[115] In some jurisdictions, banking supervisors are given the statutory authority to directly supervise third-party service providers or activities provided by third-party service providers to banks, such as the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg and the Saudi Arabian Monetary Authority (SAMA). *Id.* at 37.

[116] For example, the OCC recognized in its Frequently Asked Questions to Supplement OCC Bulletin 2013-29, "[w]hile collaborative arrangements can assist banks with their responsibilities in the life cycle phases for third-party risk management, each individual bank should have its own effective third-party risk management process tailored to each bank's specific needs." Office of the Comptroller of the Currency, *supra* note 55.

[117] *See* Part II. A to D.

[118] Inst. of Int'L Fin., *supra* note 37, at 2-5.

[119] *Id*. at 3.

Therefore if the regulation rests all oversight costs with the outsourcing financial institution and applied "[w]ith an expanded scope (such as a blanket approach that treats all cloud deployments the same), firms can lose this ability, and instead end up with maximum controls applied to all situations."[120] If financial institutions find it difficult to employ such "maximum controls', it is likely they will choose not to engage in the outsourcing relationship in the first place. Inconsistent regulatory requirements across the globe may also disincentivize financial institutions from engaging in fintech-era collaborations. As the same IIF paper pointed out, "[s]everal internationally-active firms have identified that while they have succeeded in meeting the requirements of their 'home' regulator for cloud, other barriers or asymmetrical treatments have prevented implementation in 'host' markets… **This undermines the value proposition for cloud implementation, if the benefits of enabling enhanced analytics cannot be realized across the institution's full group[emphasis added]**."[121] When fintech-era collaborations become more frequent and diverse, the regulatory dynamics facing financial institutions will get more complex and may further discourage them away from collaborating with other institutions.

At least two immediate drawbacks will arise if financial institutions are discouraged from collaborating with one another or with fintech innovators due to difficult-to-manage compliance risks. First, the greatest potential fintech holds is in its ability to promote financial innovation and inclusion. If financial institutions only develop fintech solutions in their own capacity, then they may confine themselves in the traditional way of doing business and fail to respond to consumers' needs effectively.

Second, if fintech innovators and tech giants do not have sufficient experience collaborating with financial institutions, they will not fully understand how financial institutions and their regulators think. Fintech-era collaborations serve as wonderful opportunities for nonfinancial firms to learn how financial regulation works and to adapt themselves to the existing financial regulatory framework more quickly. If these opportunities are wasted, it means the regulators will have to put extra effort to bring these fintech firms into compliance with their regulatory authority. These situations contradict with the regulatory implications learned from the preceding analysis as they will undermine the regulators' capability and capacity to learn and prevent them from challenging and redefining current regulatory parameters.

To effectively address these issues, this paper argues that regulators need to find a way to oversee and regulate risks arising from collaborations between financial institutions and nonfinancial firms, and at the same time, try promoting such collaboration to its fullest extent. The existing outsourcing regulation is not in the best position to achieve that mission and therefore there presents a need for introducing a novel regulatory approach. Such an approach, as Part III will show, can build on the innovative use of "industry sandboxes," an idea that is gaining attention only recently. In Part III, the author will explain how industry sandboxes work and how can regulators, by actively engaging themselves in the sandboxes, shift the existing regulatory regime to a collaborative data-empowerment supervisory environment.

III. FROM INDUSTRY SANDBOX TO SUPERVISORY CONTROL BOX

This Part begins by introducing the concept of industry sandboxes and analyzes the

[120] *Id*. at 3-4.
[121] *Id*. at 4.

benefits and challenges using these sandboxes. It then distinguishes industry sandboxes further into narrow-purpose sandboxes and broad-purpose sandboxes, and advocates that regulators should participate actively in broad-purpose sandboxes, developing SupTech solutions, and then utilizing SupTech to turn these sandboxes into "supervisory control boxes" based on which a collaborative data-empowerment supervisory regime can be made a reality.

A. Industry Sandbox

One can trace the root of the industry sandbox concept back to the Financial Conduct Authority's (FCA) Regulatory Sandbox report published in November 2015. The FCA proposed the idea of the virtual sandbox and sandbox umbrella, which set out two possible forms for industry-led sandboxes. A virtual sandbox means "cloud-based solution set up and equipped in collaboration between the industry, which businesses then could customise for their products or services, run tests with public data sets or data provided by other firms […], and then invite firms or even consumers to try their new solution."[122] The FCA perceives that a virtual sandbox could be introduced by the industry and functions as "an environment to enable firms to test their solutions virtually without entering the real market."[123] A sandbox umbrella, on the contrary, will operate in the real market and "would need to be authorised with appropriate permissions and then supervised by the FCA"[124] on behalf of unauthorized innovators who offer their services under the umbrella's shelter.[125]

In April 2016, the FCA went further and invited Innovate Finance, an independent, not-for-profit membership association representing the UK's FinTech community, to chair an industry consultation to explore the feasibility and operability of industry-led sandboxes. Innovate Finance conducted the consultation during July 2016 and April 2017 and published a full set of findings and recommendations in May 2017.[126] The report on final consultation findings ("Final Consultation Report") names these industry-led sandboxes as Industry Sandbox and define it as "a shared off-market development environment where developers of FinTech solutions can access data, technologies, and services from different providers in order to validate innovative ideas or address common industry challenges."[127]

The Final Consultation Report 's definition seems to confine an industry sandbox's operation to an "off-market environment," but recognized that an industry sandbox's participants could range very widely from FinTech startups, financial institutions, technology vendors, professional services firms, venture capital funds, regulators, academia and professional membership bodies.[128] From the sample types of industry sandboxes identified by the Final Consultation Report, the term industry sandbox is in effect loosely defined to include various industry-led initiatives such as API and data marketplaces, software deployment platforms and platforms for shared resources.[129]

Despite a rather loose definition, the consultation findings suggest that any industry

---

[122] FIN. CONDUCT AUTH., REGULATORY SANDBOX 12 (Nov. 2015).
[123] *Id*.
[124] *Id*. at 13.
[125] *Id*.
[126] Home page of Industry Sandbox, available at https://industrysandbox.org/ (last visited Dec. 30, 2018)
[127] INDUSTRY SANDBOX CONSULTATION, A DEVELOPMENT IN OPEN INNOVATION – INDUSTRY SANDBOX CONSULTATION REPORT 4 (May 2017).
[128] *Id*.
[129] *Id*. at 54-56.

sandbox should follow the following design principles: be able to validate innovative ideas, be open and accessible to any groups within the fintech ecosystem, be self-sustainable and operated by the industry members, and be able to operate in a neutral and safe fashion.[130] Salient examples of industry sandboxes include Boston Fintech Sandbox and Bill Melinda Gates Foundation's Level One Project.[131] Some Chinese blockchain initiatives also claim themselves as blockchain industry sandboxes, such as the Taishan Sandbox launched by Andrew International Sandbox Research Institute in December 2017.[132] Some also refer to FinTech Delivery Panel's[133] Guide on *Supporting Fintechs in Engaging With Financial Institutions* as a similar form of industry sandbox as the Guide aims to facilitate standardized interactions between fintech firms and financial institutions.[134] It is fair to say that Industry Sandbox could be very broadly defined to refer to a *semi-open*[135]*, membership-based platform where firms, regulators and academia can share data, exchange resources, develop technologies and explore solutions in a controlled environment."*

There are multiple benefits to using industry sandboxes. First, industry sandboxes can serve as a co-working space for firms who aim to adopt innovative technologies, identify common problems and explore possible solutions as a given technology will be frequently and thoroughly tested. Most importantly, the cost for testing will be equally shared among sandbox members and therefore reduces the likelihood of one firm piggybacking on the other firm's efforts. Firms can achieve scalability of using certain technology much easier as more firms will be familiar with the technology's potential uses and limits and develop commonly acceptable technical and application standards together.

Second, industry sandboxes facilitate extensive collaboration between financial institutions and nonfinancial firms and thus help them identify possible operational and third-party risk which would be generally uncovered in a real-life situation. In addition, such financial-nonfinancial-partnership model benefits both the small start-ups and larger financial firms. It gives start-ups access to a larger consumer base and enables financial firms to "innovate and improve products at a faster pace, without having to go through the full development process themselves."[136] Large financial firms' experiences with regulatory sandbox have shown that "the process of setting up their test with a partner often identified ways to improve their own procurement and governance processes for on-boarding start-ups."[137] Industry sandboxes enable similar collaborative tests and thus is likely to achieve similar effects for financial firms.

---

[130] *Id*. at 26.

[131] For how these two sandboxes work, *see Id*, at 54.

[132] Tien De Sin Liang (天德信链), *World's First Blockchain Industry Sandbox, Launches in China*, Jan. 26, 2018, available at http://vlambda.com/wz_wBjQKycvrz.html (last visited Dec. 29, 2018).

[133] The FinTech Delivery Panel is chaired by HM Treasury's Special Envoy for Fintech and was launched at the request of the Treasury to deliver initiatives and ideas that would help promote the growth of the fintech sector in the UK. It includes leading fintech entrepreneurs such as representatives from Onfido, TransferWise, Starling Bank, FreeAgent, the ID Company, MarketInvoice, Monzo, The Channel Syndicate and World Remit, together with representatives of some of the UK's biggest banks and insurance companies such as Barclays, Lloyds Banking Group, RBS, HSBC, Santander and Aviva. Tech City UK, *Tech City UK sets up 'Fintech Delivery Panel'*, FINEXTRA, Sept. 13, 2017, available at https://www.finextra.com/pressarticle/70669/tech-city-uk-sets-up-fintech-delivery-panel/wholesale (last visited Dec. 29, 2018)

[134] This is based on the author's meeting with staff at Innovate Finance in June 2018.

[135] Semi-open in a sense that member firms develop and test solutions together in a close environment but the sandbox membership is nonetheless open to new entrants.

[136] Fin. Conduct Auth., *supra* note 19, at 17.

[137] *Id*.

Third, industry sandboxes create a platform based on which different firms can safely and efficiently share data as firms can obtain customers' consent collectively and effectively address customers' concern.

Fourth, industry sandboxes allow regulators to more closely observe the industry's use of new technologies, practices, and standards in a controlled environment and further develop proper regulatory responses to challenges arising from it.

Fifth, a membership-based industry sandbox where industry players can conduct commercial and technical experiments would reduce the need to resort to regulatory experimentations and thus save significant regulatory and supervisory resources.

Last but not least, industry sandboxes would enable the firms in different countries to conduct cross-border experiments in a cloud-based environment. Cross-border trials increase firms' ability to "scale new technologies in multiple jurisdictions"[138] and in turn develop cross-border applications that can satisfy consumers' needs for cross-border financial services or solutions. A cross-border industry sandbox can also provide the regulators with the data needed to inform the licensing or authorization processes and further reduce entry barriers to the market for newcomers.[139] Of course, a cross-border industry sandbox will only work if there exists sufficient level of collaboration among regulators across borders. A global sandbox as proposed by the Global Financial Innovation Network, if eventually formed, would facilitate the operation of cross-border industry sandboxes by providing clarity on regulators' expectations about firms' use of innovative technologies and novel business models.[140]

The use of industry sandboxes does not come without challenges or problems. This paper highlights the two most important issues. First, some industry sandboxes may function as champions or promotors for certain industry or technical standards and the existence of multiple standards may prevent different sandboxes from interoperating with each other. The lack of interoperability makes emerging technologies difficult to scale and thus increases end consumers' costs of using those technologies. Firms in different sandboxes have the incentive to expand the membership to its fullest extent to create a network effect for members and their respective customers. Once an industry sandbox creates network effects for its members, those who cannot join the sandbox will have less competitive advantages comparing to members in the sandbox.

Second, collaborating with other firms in an industry sandbox will likely subject financial institutions to third-party risks and operational risks. If there lacks an effective governance framework for stakeholders in the sandbox to manage risks and liabilities, most firms will prefer industry sandboxes to operate only in an off-market environment and involve little or no exchange or sharing of customer data as such a narrow-purpose sandbox will help limit the scope and scale of potential liability. For example, banks can explore the benefits and risks of implementing open banking solutions with multiple third-party service providers in an industry sandbox. There are various things banks and third-party service providers (TSP) can collaborate to explore and design, such as data formats, open APIs standards, cyber security standards and TSP governance process. However, only when banks and TSPs are testing their proposed standards or process in a real-life scenario and exchanging real customer data can they actually know whether their proposed solutions are viable and can sustain in a live market. If the regulatory regime facing the banks and TSPs are not clear in terms of what data can be shared and which party needs to take ultimate liability when there

[138] Abu Dahbi Global Market et al., *supra* note 21, at 11.
[139] *Id*. at 11-12.
[140] *See Id*.

occurs a data breach during the process of sharing, institutions, in particular banks, are very unlikely to engage in a live-market industry sandbox and thus hinders the sandbox' potential to identify and locate adequate open banking standards. To sum up, narrow-purpose industry sandboxes might serve well the role of *resource-sharing platforms* and *technology-testing grounds* but may not ideally undertake the role of *accelerators for risk governance and regulatory solutions*. In other words, narrow-purpose sandboxes only partially solve commercial or technological problems but leave other problems that are integral to business and industrial development to the future or separate initiatives. As two seasoned fintech specialists advocated in a recent piece,

> "the ideal sandbox solution should aim to address the shortcomings of the existing and fragmented approach to the banking sandbox environment. It should be a multi-bank API sandbox operated by a standalone institution that works with the various stakeholders as partners. Taking the leading global standards, it should enable partners to accelerate the creation and to facilitate the management of a fintech ecosystem, underpinning the next generation of financial technology. A focused, partner-supported initiative has the best chance of delivering an industry-standard cross-bank sandbox solution, capable of addressing the problems outlined in this paper. It would enable developers to quickly implement innovative financial services solutions that span across multiple financial organisations, test them with production-grade test data reflective of real-life customer segment, and quickly deploy them into production." [141]

Intra-and-inter sandbox interoperability, *accessibility to live customer data*, and *agility to bring solutions to consumers* are probably the most crucial features which enable an industry sandbox to develop its potential to the fullest extent. Following similar belief, this paper argues that the regulators should encourage the use of these types of industry sandboxes and to turn them into mechanisms to achieve a balance of regulation and promotion of fintech-era collaborations.

B. The Role of Regulators and SupTech

This paper's perception of industry sandboxes follows the descriptions of the Final Consultation Paper but differs in two major aspects. First, the paper argues that industry sandboxes can operate both in off-markets and real live markets. Players in an industry sandbox can have access to live customer data and the solutions developed in the sandbox can be directly offered to consumers and be fine-tuned based on real customers' feedback. Under this definition, the operation of industry sandboxes may pose consumer, market integrity and stability risks, and thus a regulatory solution is needed.

Second, this paper argues that regulators should actively engage with industry sandboxes just like in a regulatory sandbox scenario. Regulators should not just act as observers and have access to outputs from the industry sandbox[142]. Rather, regulators can closely monitor activities in the sandbox and craft an ideal governance regime collectively with the sandbox members. For example, in an industry sandbox where

---

[141] Etienne Castiaux and Anatoli Arkhipenko, *Fintech Sandboxes: Bring Your Own Sand*, FinTech Futures, available at https://www.bankingtech.com/2018/06/fintech-sandboxes-bring-your-own-sand/ (last visited Dec. 29, 2018)

[142] *Id*. at 26.

participants are working together to operate blockchain-enabled solutions such as supply chain finance, cross-border remittance or syndicated loans, regulators can choose to play the role of an auditor node[143] and conduct real-time monitoring of activities in the sandbox. We have not seen any regulators playing such a role in a distributed ledger structure, but the benefit of doing so is obvious as regulators will be able to not only timely supervise transactions but also cultivate their capability to utilize new technologies. This paper refers to sandboxes with the foregoing features (e.g., regulators' active involvement) as *broad-purpose industry sandboxes*.

The analysis of fintech-era collaborations and their respective regulatory implications have called for a novel regulatory system.[144] This paper terms such a regulatory system the *collaborative data-empowerment supervisory regime*. Such a regime empowers both the regulator and industry by enabling safe and efficient intra-industry, inter-industry and industry-regulator data-sharing and collaborative learning. It also harnesses both the regulatory and industry wisdom to explore an effective risk governance framework and enabling regulatory approach. As fintech-era collaborations deepen, diversify and become more frequent and complex, traditional outsourcing regulation is likely to fail to respond effectively to risks and challenges that arise. The financial regulator needs to think more creatively and engage with the industry more actively. Broad-purpose industry sandboxes, as this paper argues, present the regulator with a wonderful opportunity to fulfill a collaborative data-empowerment supervisory regime. This so-called collaborative data-empowerment supervisory regime, as will be explained further in later this Section and Section C of this Part, goes beyond the current scope of industry-regulator collaborations in which multiple stakeholders exchange information and shape regulations.[145] Such a regime, empowered by regulators' use of supervisory technologies and enabled by regulators' participation in board-purpose industry sandbox, would allow the constant and real-time flow of supervisory data from the industry to the regulator and let regulators take immediate actions in the form of machine-executable rules.

Having regulators cooperate with the industry is by no means a novel idea to financial regulation. The industry is often empowered by the authority to regulate itself or cultivate its own behavioral standards. Many financial institutions work with regulators intensively through active advocating activities. Despite the above, some proponents for industry-regulator collaboration such as the New Governance theorists still consider the status quo does not amount to an ideal manifestation of public-private collaboration.[146]

Effective public-private collaboration should not only lever the self-disciplinary power of the industry to facilitate regulatory objectives but also effectively channel the regulatory authority and resources to areas where the industry's self-disciplinary power

---

[143] Auditor node refers to "node permissioned to view the ledger but not make updates". COMM. ON PAYMENTS AND MARKET INFRASTRUCTURE, DISTRIBUTED LEDGER TECHNOLOGY IN PAYMENT, CLEARING AND SETTLEMENT - AN ANALYTICAL FRAMEWORK 5 (Feb. 2017).

[144] *See supra* Part II. E.

[145] Such as negotiated rulemaking and the notice and comment procedures in the American Administrative Law.

[146] Famous scholarly works on New Governance and financial regulation, s*ee e.g.,* Annelise Riles, *Is New Governance the Ideal Architecture for Global Financial Regulation?* 31 MONETARY & ECON. STUD. 65 (2013); Saule Omarova, *Wall Street as Community of Fate: Toward Financial Industry Self-Regulation,* 159 U. PA. L. REV. 411, 438 (2011); Cristie Ford, *New Governance in the Teeth of Human Frailty: Lessons from Financial Regulation,* 2010 WIS. L. REV. 441 (2010); Cristie L. Ford, *New Governance, Compliance, and Principles-Based Securities Regulation,* 45 AM. BUS. L.J. 1 (2008).

fails to function.[147] The Global Financial Crisis of 2008 has provided several good case studies of regulators failing to exercise external check to properly channel the industry's self-disciplinary power. Salient examples include the Internal-Rating Based model under the Basel II accord and the Consolidated Supervised Entity regime adopted by the SEC. Indeed, the pre-Crisis experiences have shown that "regulators may actually have been too deferential, and too reliant on the industry's self-correcting and innovating powers."[148] As Professor Ford observed, regulators may have "abdicat[ed] their responsibility where they implement flexible, iterative, collaborative systems without simultaneously developing mechanisms to 'kick the tires' on industry-generated solutions."[149] All of the above underscores the importance of channeling the industry's self-disciplinary power through the timely and proper exercise of regulatory authorities and resources. This would require transparent and sincere exchanges of information and thoughts by regulators and the regulated as well as a mutually-trusted environment which allows continuous learning and iterative testing on both sides.[150]

Some might argue that close regulator-industry collaboration will subject financial regulators to greater regulatory capture[151] and thus further undermine the supervisory effectiveness. Regulatory capture is indeed an intricate issue and is probably rooted by the asymmetry between the financial industry and the regulators' institutional and political power.[152] Regulatory capture in financial regulation, to some degree, is inevitable as we "depend on constant interaction between the industry and regulators" and "we would want some degree of coordination between government and banks for the implementation of monetary policy and the maintenance of financial stability."[153] Therefore the solution lies in how can we promote "principles for maintaining transparency and accountability" "when the degree of influence by one legitimate stakeholder in the regulatory process over another has become unbalanced."[154] As Professor Baxter proposed, these principles can be categorized into five strategies: "adequate regulatory capacity; meaningful transparency; meaningful access by stakeholders; external checks; and internal checks [within the industry itself]."[155] A close examination of the five strategies will find that the key lies in whether the regulator has sufficient data and capacity and whether the industry has meaningful access to the formation of regulation and a self-constraint culture. Among these things, the author would argue that access to meaningful and prompt data plays the most important role as data empowers regulators' supervisory capacity and informs their regulatory making, which will significantly enhance transparency and accountability. Therefore, ideal regulator-industry collaboration should also empower the regulators with genuine and prompt data which can provide real insights into the industry members'

---

147 *See* Cheng-Yun Tsang, *Balancing the Governance of the Modern Financial Ecosystem: A New Governance Perspective and Implications for Market Discipline*, 40 HOUSTON J. INT'L L., 531 (2018).
148 *Id*. at 576.
149 Cristie Ford, *Macro-and Micro-Level Effects on Responsive Financial Regulation*, 44 UBC L. REV. 589, 625 (2011).
150 *See Id*.
151 For the issues concerning regulatory capture in financial regulation and an insightful observation about the connections between the financial industry and the regulators, *see* Lawrence G. Baxter, *Capture in Financial Regulation: Can We Redirect It Toward the Common Good?*, 21 CORNELL J. L. & PUB. POL'Y 175 (2011).
152 *See Id.* at 119-200.
153 Lawrence G. Baxter, Understanding Regulatory Capture:An Academic Perspective from the United States in MAKING GOOD FINANCIAL REGULATION - TOWARDS A POLICY RESPONSE TO REGULATORY CAPTURE 34 (Stefano Pagliari, ed., 2012)
154 *Id*.
155 *Id*. at 35.

intentions and behaviors. A collaborative data-empowerment supervisory regime fits squarely with those requirements, especially in the era of fintech.

The arrival of the fintech era brings opportunities to the financial regulator alone with challenges. One of the greatest opportunities is the possibility to use technologies to upgrade supervisory tools and improve supervisory efficiency. These applications of technologies and adoption of fintech solutions by supervisory authorities are referred to as Supervisory Technology or "SupTech."[156] The UK's Government Office for Science first mentioned the idea of SupTech, back when it was typically embraced within "RegTech" (Regulatory Technology) and defined as "technologies that can be applied to or used in regulation, typically to improve efficiency and transparency in regulatory systems."[157][158] Later discussions and literature gradually distinguish the use of the two terms.

Broadly speaking, RegTech assists regulated institutions in complying with laws and regulations[159], whereas SupTech enables financial regulators to more effectively and efficiently carry out supervisory missions and oversight.[160] RegTech emphasizes on the ability of the regulated institutions to understand the regulatory position and interact with regulators during the compliance process,[161] whereas SupTech focuses on the need to improve the efficiency and quality of the supervisory process and regulatory rulemaking.[162] Though still at an early stage, many authorities have developed and started various SupTech solutions.[163]

The use of SupTech holds enormous potential to drive the existing financial regulatory system into a new paradigm of technology-enabled supervision. Such a regime, as recent researches suggest, will enable real-time monitoring of risks and anomalous activities, dynamic and proactive supervisory actions, automated implementation of regulatory measures, and evidence-based t normative requirements and regulatory measures.[164] Nevertheless, all of these promises will not come true unless the regulators change the way they currently deal with data and regulatory reporting.

Regulators should be able to effectively and automatically access quality data from supervised institutions and generate indicators according to different supervisory requirements.[165] Having such an ability means the supervisory data management

---

[156] FIN. STABILITY BD., ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN FINANCIAL SERVICES - MARKET DEVELOPMENTS AND FINANCIAL STABILITY IMPLICATIONS 36 (Nov. 2017); BASEL COMM. ON BANKING SUPERVISION, SOUND PRACTICES - IMPLICATIONS OF FINTECH DEVELOPMENTS FOR BANKS AND BANK SUPERVISORS 43 (Feb. 2018).

[157] UK GOV'T CHIEF SCI. ADVISER, FIN TECH FUTURES - THE UK AS A WORLD LEADER IN FINANCIAL TECHNOLOGIES 62 (Mar. 2015).

[158] For academic literature analyzing RegTech, *see, e.g.*, Lawrence G. Baxter, *Adaptive Financial Regulation and RegTech: A Concept Article on Realistic Protection for Victims of Bank Failures*, 66 DUKE L.J. 567 (2016); Arner et al., *supra* note 17.

[159] Basel Comm. on Banking Supervision, *supra* note 156, at 35.

[160] *Id*.

[161] Fin. Stability Bd., *supra* note 156, at 35.

[162] FIN. CONDUCT AUTH., FEEDBACK STATEMENT, CALL FOR INPUT ON SUPPORTING THE DEVELOPMENT AND ADOPTERS OF REGTECH 10 (2016).

[163] For a recent study on the early use cases of SupTech around the world, *see* Dirk Broeders and Jermy Prenio, *Innovative Technology in Financial Supervision (Suptech) – The Experience of Early Users*, 9 FSI INSIGHTS ON POLICY IMPLEMENTATION (July 2018).

[164] Cheng-Yun Tsang, *A Tentative Analytical Framework and Developing Roadmap for SupTech*, 37 MGMT. REV. 105, 109-110 (2018); *See also* Arner et al., *supra* note 17, at 395; TORONTO CTR., FINTECH, REGTECH AND SUPTECH: WHAT THEY MEAN FOR FINANCIAL SUPERVISION 12-13 (Aug. 2017).

[165] Tsang, *Id*. at 108-109.

model needs to shift from template-based reporting to an input-based approach.[166] An input-based approach would allow financial regulators to conduct evidence-based evaluation accurately and to exchange data with other relevant agencies effectively.[167] As the Toronto Centre rightly observes, "[r]egulatory reporting is the core of supervisory analytics and improving it should be the starting point of SupTech to create a solid basis for any advanced analytics."[168] An input-based regulatory reporting regime would save a lot of compliance costs for the supervised institutions and allow regulators to treat every institution differently based on their risks and self-governance ability.

C. From Industry Sandbox to Supervisory Control Box

This paper argues that by engaging actively and sensibly in broad-purpose industry sandboxes, regulators can gradually enable an input-based approach and develop SupTech solutions, and then further utilize SupTech to turn these sandboxes into "supervisory control boxes" and fulfill a collaborative data-empowerment supervisory regime. The reasons are as follows.

First, as researchers have identified, major challenges to implementing SupTech include the existence of data silos at regulatory agencies and regulated institutions and the lack of budgetary resources to procure and develop SupTech solutions.[169] Broad-purposes industry sandboxes provide a forum for different players across industry boundaries to exchange data. This efficient and controlled way of data exchange gives the regulators access to a one-stop supply of data from different use cases, institutions and even industries. If such data supply can be in a standardized and machine-readable format, then it would save regulators' a lot of resources in collecting and analyzing data. Due to resource constraint, regulators usually encounter difficulty in retaining qualified professionals and in-house expertise.[170] Participating in industry sandboxes allows regulators to benefit from expertise supplied in the sandbox and *de facto* lever these resources without overburdening regulatory budgets.

Second, it is also suggested that "the lack of inter-departmental and inter-agency coordination for integrating needs that could be addressed by a single SupTech solution"[171] has prevented SupTech from taking off. Broad-purpose sandboxes provide an informal but effective forum for inter-agency communication and coordination as regulators from different agencies would generally be more comfortable and genuine in a controlled testing environment and especially when they are learning, instead of performing duties, together.

Third, risks arising from the use of SupTech may have a negative impact on the regulator's effectiveness and reputation.[172] These risks include "erroneous outputs from ill-designed algorithms," data and cybersecurity risks, third-party risks, and the "potential for third-party manipulation of big data used as input for SupTech."[173] Engaging and collaborating actively with industry members in broad-purpose

---

166 Toronto Ctr., *Id.* at 11; OFFICE OF FIN. RESEARCH, DEVELOPING BEST PRACTICES FOR REGULATORY DATA COLLECTIONS 9 (2016).
167 Tsang, *supra* note 164, at 109.
168 TORONTO CTR., SUPTECH: LEVERAGING TECHNOLOGY FOR BETTER SUPERVISION 11 (July 2018).
169 *Id*. at 10.
170 *Id*.
171 *Id*.
172 *Id*.
173 *Id*.

sandboxes allow regulators to explore effective ways for managing the risks and consequences of algorithm discrimination, data security, cyber-attacks and third-party operational failures as repetitive tests can be conducted in the sandbox and collective learning will take place very frequently. Knowledge learned from a sandbox can also spill over to other industry sandboxes as regulators can take part in every sandbox and serve as a knowledge bridge and diffusion catalyst.

As regulators have more experience collaborating with different types of institutions in industry sandboxes, they can direct the standardization of data formatting, sharing and reporting based on lessons learned. This would enable interoperability among different industry sandboxes and diffusion of best practices on risk governance and liability management framework. Regulators then further turn these industry sandboxes into what this paper termed as "supervisory control boxes." The supervisory control box symbolizes a new paradigm of technology-enabled self-regulation, which essentially allows sandbox members to regulate themselves through a collaboratively-designed-and-maintained governance framework.

In the control box, regulators facilitate (but not dominate) the crafting of an effective governance framework, set common standards for regulatory reporting data sharing, develop SupTech solutions and apply them to sandbox members to gather user feedback. Regulators can also employ machine-executable rules to enable automated regulation in the sandbox, and conduct real-time monitoring of sandbox members as envisaged by advocates such as Andrew Haldane.[174] Regulators might also empower consumers with rights to data portability using technologies such as distributed ledgers and biometrics. With the availability of infrastructures for data portability and interoperability, consumers can freely decide whether and what to share with which industry sandboxes, and financial institutions and nonfinancial firms can deepen fintech-era collaborations and develop solutions that better satisfy consumers' needs.

The supervisory control box can cure the weaknesses of the existing outsourcing regulation. Each control box can form a governance body subject to the regulator's direct supervision. One can perceive this design as a way for the regulatory authority outsourcing some of its supervisory missions, functions, and activities to the governance body and hold the body accountable for the members' compliance with the regulatory requirements.

Outsourcing arrangements and TPS relationships can take place with fewer compliance costs in the control box. Because financial institutions can collaborate and share costs of meeting responsibilities for managing a relationship and large or foreign-based service providers will be more willing to accept standardized contractual terms in a control box as they can build up a relationship with many financial institutions all at once and subject to one set of supervisory and examination requirements. For example, the governance body in a control box can play the similar role of TruSight, a collaborative initiative by five largest banks in the US which aims to "streamline and simplifies third-party assessments by executing best practice assessments once and delivering to many."[175]This new model for outsourcing regulation and TPS relationship

[174] Andy Haldane, Speech at the Maxwell Fry Annual Global Finance Lecture: Managing Global Finance as a System, Birmingham University 10 (Oct. 29, 2014); *See also* Stefano Battiston et al., *Complexity Theory and Financial Regulation*, 351 Science 818, 819 (2016) (advocating that "[o]ne ambitious option would be an online, financial-economic dashboard that integrates data, methods, and indicators. This might monitor and stress-test the global socioeconomic and financial system in something close to real time, in a way similar to what is done with other complex systems, such as weather systems or social networks.")

[175] TruSight's website, available at https://trusightsolutions.com/ (last visited Jan. 1, 2019)

governance will encourage financial institutions to more actively and frequently collaborate with small fintech start-ups and giant technology services providers, either domestically or internationally, in various situations.

Of course, some may raise concerns that active and frequent participation in these control boxes also consumes a significant amount of regulators' resources, and the regulators might not necessarily have motivations to do so as they face little reward and might be blamed if something goes wrong. But the author would argue that even if in the absence of these sandbox or control box activities, financial regulators still need to tackle risks and challenges posed by these fintech-era collaborations on a day-to-day basis. They will have to either consider to grant full permission or limited authorization for each individual collaboration or spend separate efforts to monitor risks for each collaborative initiative. In the supervisory control box, regulators can treat the governance body as a portal and single point of entry, which allows them "access to all the tools necessary to interact with multiple financial institutions seamlessly."[176] This model would in fact save regulatory and supervisory costs that arise from increasing fintech-era collaborations in the long-run. To be sure, the lack of regulatory resource has been a global issue that needs to be resolved to urgently. The problem will only get worse when more fintech firms join the market and greater collaboration taking place between financial institutions, fintech start-up and bigtech companies. The legislative branch should consider seriously whether to equip its regulators with an abundant budget so as to respond to daily challenges arising at both the domestic and the global level. As for the concern that regulators might not have the incentive to take part in sandbox or control box activities, the rapid, worldwide adoption of the regulatory sandbox mechanism seems to have suggested otherwise. According to a recent survey conducted by the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA) and Cambridge Centre for Alternative Finance (CCAF) at the University of Cambridge Judge Business School, "regulatory sandboxes now live or planned in over 50 jurisdictions."[177] Among these 50 jurisdictions, the regulatory sandbox has been operational in 31 jurisdictions.[178] Given the world's first regulatory sandbox regime was only launched in June 2016 by the UK, the diffusion and adoption rate is quite impressive and probably shows how motivated worldwide financial regulators are when it comes to the regulation of fintech.

Supervisory control boxes, if they become a reality, can empower both the regulator and industry with effective data-sharing and collaborative learning and move the regulatory system toward a collaborative data-empowerment supervisory regime.

IV. A TENTATIVE ROADMAP FOR FUTURE REFORMS

The creation and wide adoption of supervisory control boxes would certainly take a long time. Both the regulator and industry have a lot to do to speed up the arrival of such a new paradigm of data-empowered supervision. This paper proposes a roadmap composed of three major steps for policymakers and regulators to push for future reforms.

[176] Castiaux and Arkhipenko, *supra* note 141 .
[177] UNSGSA &CCAF, EARLY LESSONS ON REGULATORY INNOVATIONS TO ENABLE INCLUSIVE FINTECH: INNOVATION OFFICES, REGULATORY SANDBOXES, AND REGTECH 26 (Feb. 2019).
[178] *Id*. at 52-53.

A. Digitalizing and Standardizing Regulatory Reporting

The regulators can start by digitalizing and standardizing regulatory reporting with an aim towards achieving the automation of the entire supervisory process. Some countries are currently working on this front. For example, the House of Representatives in the US proposed the Financial Transparency Act[179] to require financial supervisory agencies to change their current regulatory reporting management so as to ensure the flow of regulatory reporting will be searchable, standardized, and machine-readable in the future.[180]

Austria presents another salient example. The Austrian central bank, OeNB, in 2014, cooperated with seven leading banks in the country to jointly establish the Austrian Reporting Services GmbH (AuRep). AuRep adopts a software system provided by BearingPoint [181] and functions as a centralized reporting platform to bridge communication of regulatory data between the member banks and OeNB. Under this structure, banks only need to upload original data to this platform through a standardized format, and then OeNB can pull the basic datasets in the platform and construct them into smart datasets based on its supervisory needs. [182] This approach allows banks to meet different regulatory information requirements through one-time data submission.[183]

Some might well argue that standardized reporting regimes will lead to increased compliance costs for firms and therefore, potentially limit firms' market entry. The author shares this sentiment, but even though it requires upfront IT Investments by firms to implement standardized regulatory reporting, firms will find their long-term compliance costs reduced as they can save lots of time and money producing reports to satisfy different format and standard requirements. Moreover, standardized regulatory reporting facilitates regulators' use of data and data analytics. Most importantly, many financial institutions have already digitalized and automated their internal process for generating regulatory and supervisory reports. If regulators can also digitalize and standardize their end of data acceptance and processing then financial institutions can save tons of reporting and compliance costs and be further incentivized to engage in data-sharing activities.

B. Cultivating Technology-Empowered Regulators

The second step calls for enhancing the regulators' technology literacy and capability. As the Toronto Centre rightly observed "[p]aradigm shifts can only succeed with the right mindset and leadership at regulatory and supervisory authorities since they require a profound cultural transformation. Authorities need first to recognize that they must change and be strategic in reviewing existing approaches, organizational structures, IT systems, and technical skills." Only when regulators' have a sufficient level of technical skills, they can wholeheartedly embrace the use of SupTech solutions

[179] It later became a bipartisan proposal.
[180] Daniel Morgan, Sameer Gulati, Laura Biddle and Loyal Horsley, *The Future of RegTech for Regulators – Adopting a Holistic Approach to a Digital Era Regulator*, TRANSATLANTIC POLICY WORKING GROUP FINTECH (TPWG) 17 (June 2017).
[181] It is a RegTech solution provider and multinational management consulting firm headquartered in Amsterdam, Netherlands.
[182] Morgan et al., *supra* note 180, at 12.
[183] Tsang, *supra* note 164, at 115.

and develop trust in the technology-enabled supervisory regime.

To build a sufficient level of technology capability on the side of regulators, many factors matter. For example, the institutional structure and organizational culture of the regulatory agency should encourage staffs to keep learning and provide them with proper incentives such as a possible promotion or extra compensation.[184] The legislative branch, on the other hand, should equip and empower financial regulators with abundant fiscal resources. With the rapid advancement in innovative technologies, the resource imbalance between financial regulators and the regulated institutions has become larger.[185]

Financial institutions can compete for best talents in the market and across the globe with handsome compensation packages, whereas the regulators can only attract talents who are willing to accept lower compensation. Regulatory agencies should enjoy a greater budget, sufficient financial resources, and flexible compensation arrangements to empower their staffs with stronger technological literacy and capacity.

If these developments sound too remote or too unrealistic in the short run, there are two alternative solutions based on which regulators can be more tech-powered. Firstly, many global standards-setting bodies (G-SSBs) or international financial organizations are aware of the insufficiency of regulators' technology capability and have been offering training sessions or other institutional supports. For example, the Toronto Centre provides various practical training to financial sector supervisors in emerging markets and low-income countries.[186] The Bank for International Settlements ("BIS") has just established a BIS Innovation Hub to foster worldwide collaboration on innovative financial technologies within the global central banking community.[187] Worldwide regulators can cooperate via G-SSBs to develop more public goods like the abovementioned in the fintech space, and create expertise-codeveloping networks to empower each other's technology proficiency.[188] Secondly, regulators can cooperate in conducting cross-border trials on the use of new technologies. In fact, some regulators are doing so already. For example, the Bank of Canada and the Monetary Authority of Singapore have recently collaborated on the Jasper-Ubin project to test cross-border high-value transfer using distributed ledger technologies.[189] Through such cross-border collaborations, a regulator can lever on other regulators' resources and expertise to further cultivate its own technology capability. More than that, such collaborative initiatives will bring very positive images for the participating regulators as joining them will signal to the globe that these regulators are really trying to keep abreast of modern technologies and up-to-date industrial developments. Positive images bring a good reputation, and it will further allow the regulator to persuade its legislative branch to give them more fiscal resources.

The more technology-empowered the regulators are, the more open-minded these regulators will be when facing fintech-era collaborations and operation of industry

---

[184] Yueh-Ping (Alex) Yang and Cheng-Yun Tsang, *RegTech and the New Era of Financial Regulators: Envisaging More Public-Private Partnership Models of Financial Regulators*, 21(2) U. PA. J. BUS. L. 354-404 (2019) (discussing the conduct aspect of RegTech and emphasizing that the quality and efficiency of financial regulators should keep pace with technological developments)

[185] *See Id*.

[186] About Toronto Centre, *available at* https://www.torontocentre.org/About (last visited July 7, 2019),

[187] Bank for Int'L Settlements, *BIS to Set Up Innovation Hub for Central Banks* (June 30, 2019), *available at* https://www.bis.org/press/p190630a.htm (last visited July 7, 2019).

[188] *See Id.*

[189] For details of the Project, *see* BANK OF CANADA AND MONETARY AUTH. OF SINGAPORE, JASPER – UBIN DESIGN PAPER ENABLING CROSS-BORDER HIGH VALUE TRANSFER USING DISTRIBUTED LEDGER TECHNOLOGIES (2019).

sandboxes. They will be more willing to engage with members in industry sandboxes actively and more likely to inject greater resources to turn them into supervisory control boxes.

C. Rethinking the Outsourcing Regulation

The rationale and thinking behind the contemporary outsourcing regulation, as this paper has analyzed, builds upon certain dated assumptions.[190] These assumptions were largely driven by the dichotomy which divides licensed financial institutions and unauthorized firms into two separate groups. Either confined by the law or long-subscribed boundary-thinking, financial regulators tend to pursue regulatory objectives by imposing requirements on licensed firms. Nevertheless, the dichotomy no longer helps achieve effective supervision on fintech activities arising from extensive collaboration among firms of different types, let alone the dividing line itself has become increasingly blurred. It begs the question of whether it remains optimal to preserve regulatory thinking based on this dichotomy.

Also, these assumptions were also a result of the limit on regulatory capacity which leaves the regulators with no choices but to rely on the outsourcing regulated firm to effect supervision over its relationship with service providers. Regulatory capacity has made significant progress over the past decade thanks to rapid developments in information technologies and computing powers. With the use of SupTech, the regulator is now able to transcend its capacity limit and brings new perspectives into traditional regulatory thinking.

The third step, calls for a systemic rethinking and review of the contemporary outsourcing regulation and its regulatory assumptions. Regulators should consider the possibility of creating a novel form of regulatory outsourcing under which regulated firms collaborate with unauthorized firms to establish a sandbox-umbrella-alike governance body to perform supervisory tasks on behalf of the regulator, and to ensure compliance with regulatory requirements by the sandbox members.

If such regulatory outsourcing model becomes a reality, then regulators will be more confident when acting beyond the dichotomy of industry line and the limit of regulatory capacity. Thinking and acting outside the box would allow regulators to boldly explore and test innovative regulatory approaches such as actively participating in industry sandboxes and pushing forward a closer public-private collaboration than ever previously imagined.

V. CONCLUSION

The world of finance has marched into a fintech era in which close and diversified collaborations among financial institutions, fintech start-ups, and technology firms are taking place frequently and extensively. The most common types of these collaborations include third-party service relationships, data-sharing arrangements, regulatory experiments, and industry consortia. Each collaboration type presents different risks and governance challenges to the collaborating firms and the consumers, and most importantly, poses unprecedented challenges to the regulators and the conventional regulatory thinking.

[190] *See supra* Part II. E.

To effectively respond to these challenges, the regulatory system should:

1. enhance financial regulators' capability and capacity to learn new technologies, to collect data, and to collaborate with regulators in other industries;
2. allow the regulators to be in constant and close dialogue with the industry so as to facilitate the creation of ideal governance structure and liability framework among different stakeholders in fintech-driven collaborative initiatives;
3. enable an information infrastructure and regulatory architecture that allow data interoperability and portability in a safe manner and;
4. help regulators continuously reflect regulatory parameters and explore adequate ways to regulate fintech collaborations and nonfinancial institutions.

The current outsourcing regulation upon which regulators rely on regulating fintech-era collaborations fails to meet these requirements, and are premised on dated assumptions. We should not only rethink the role of the regulators but also reflect on the conventional thinking and rationale behind the existing regulatory framework. Financial regulators should engage actively in public-private collaborations. They can encourage the use of broad-purpose industry sandboxes and thus enable a collaborative data-empowerment supervisory regime. Such a regime, if made possible, would empower both the regulator and industry in conducting safe and efficient intra-industry, inter-industry and industry-regulator data-sharing and collaborative learning. It would also harness the regulatory and industry wisdom to explore an effective risk governance framework and enabling regulatory approach to better regulate fintech-era collaborations.

Regulators should also embrace and lever SupTech to transform industry sandboxes into supervisory control boxes. In the control boxes, regulators can help craft an effective governance framework, set standards for regulatory reporting and data sharing, upgrade SupTech solutions, and employ machine-executable rules to enable automated regulation and real-time monitoring. Outsourcing arrangements and TPS relationships can take place with fewer compliance costs in the control box, and financial institutions will be more willing to actively and frequently collaborate with small fintech start-ups and giant technology services providers, either domestically or internationally. Well-regulated fintech-era collaborations and the effective function of the supervisory control boxes will promote not only financial innovation and inclusion but also enhance regulatory capacity and capability.

Rome was not built in a day, of course. The realization of a supervisory control box remains remote for jurisdictions where regulatory reporting is not yet digitalized, and the regulatory staff is not adequately empowered by technology. Policymakers need to have a clear roadmap for future reforms and gradually shift the current regime to a new paradigm of technology-enabled regulation.