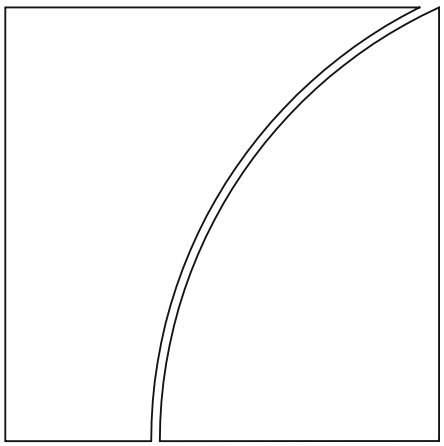
Financial Stability Institute

FSI Insights

on policy implementation

No 36



Big tech regulation: what is going on?

By Juan Carlos Crisanto, Johannes Ehrentraud, Aidan Lawson and Fernando Restoy

September 2021

JEL classification: G18, G21, G23, G28, L41, L51
Keywords: big techs, activity-based regulation, entity-based regulation, competition, data protection, data-sharing, conduct of business, operational resilience, fintech, financial stability

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-2481 (print)
ISBN 978-92-9259-505-0 (print)

ISSN 2522-249X (online)
ISBN 978-92-9259-506-7 (online)

Contents

Big tech regulation: what is going on?[1]

Executive summary

The emergence of large technology firms (big techs) represents a major source of disruption to the financial system and the economy. Big techs have expanded the available range of financial products and services, often with enhanced customer experience. However, the ease and speed with which these companies can scale up their activities and expand into finance may generate pronounced concentration dynamics. This could significantly affect the adequate functioning of the financial system and may damage market contestability and eventually increase operational vulnerabilities due to the excessive reliance of market players on the services provided by big techs.

Different jurisdictions have moved to adjust their policy frameworks to cope with the risks presented by big techs. In particular, a number of policy initiatives have emerged in China, the European Union (EU) and the United States over the last few years in the areas of competition, data protection and data-sharing, operational resilience, conduct of business and financial stability. These initiatives generally seek to achieve a balance between addressing the different risks posed by big techs and preserving the benefits they bring in terms of market efficiency and financial inclusion.

Thus far, competition has been the policy area where the most initiatives have been conducted and a paradigm shift is emerging. Given the large potential for big techs to abuse their technological and data superiority to quickly dominate different market segments and adopt anticompetitive practices, preserving market contestability has become a top priority for authorities in China, the EU and the US. Competition policy proposals include not only the augmentation of traditional ex post enforcement tools but also the creation of new big tech-specific ex ante regulatory regimes.

A number of data protection and data-sharing initiatives have been proposed. Policy initiatives across the three jurisdictions place special emphasis on personal data use and data protection. Moreover, there are relevant initiatives, particularly in China and the EU, with respect to users' data portability. This, together with emerging policy and market developments on data-sharing, seems to be paving the way to a generalised use of personal data for the provision of financial services by different types of entities.

Policy initiatives are addressing the operational resilience of big tech firms. These typically apply to big techs either as providers of financial services[2] or as third-party service providers of financial firms.[3] The operational resilience requirements in both cases intend to capture all sources of operational risk (in particular, information and communication technology risks) and expect adoption of sound risk management practices, swift response in case of disruption and continuity of critical services.

Some jurisdictions have taken meaningful policy efforts to address potential conduct issues and financial stability challenges but they do not follow an homogeneous pattern. A key development in the conduct of business area is the EU's proposed Digital Services Act (DSA). This establishes extensive requirements for very large online platforms connected with the functioning and use

[1] Juan Carlos Crisanto (Juan-Carlos.Crisanto@bis.org), Johannes Ehrentraud (johannes.ehrentraud@bis.org) and Fernando Restoy (Fernando.Restoy@bis.org), Bank for International Settlements, and Aidan Lawson (aidanlawson@hotmail.com), former Associate under the BIS Graduate Programme. We are grateful to Patrizia Baudino, Jon Frost, Leonardo Gambacorta, Elisabeth Noble and Zhu Jun for helpful comments. Christina Paavola provided valuable administrative support.

[2] See Proposed Digital Operational Resilience Act (DORA) in the EU, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684 and China's regime for financial holding companies.

[3] See DORA (above) and US Significant Service Provider Program.

of their services. As such, the DSA represents a comprehensive effort to deal with how big techs treat their customers and the information they receive. Regarding financial stability, the main regulatory development is the China financial holding company (FHC) regime. This requires all entities holding two or more types of financial institutions to be structured and licenced as FHCs (if size thresholds or other conditions are met). This effectively mandated big techs to reorganise their financial business and represents a novel entity-based regulatory approach that entails a comprehensive oversight of the activities performed by big techs through all their financial subsidiaries.

Additional regulatory responses might be needed to comprehensively address big tech risks and achieve policy consistency at the international level. Recent initiatives in China, the EU and the US constitute important steps in addressing risks posed by big techs. However, if big techs continue to gain prominence in the financial system, additional policy responses might be necessary. It is also very likely that new policy actions will largely need to follow an entity-based approach and require close cooperation between competition, data and financial authorities. Moreover, given the cross-border scope of big tech activities, enhanced international regulatory cooperation is essential.

Section 1 – Introduction

1. **Technological developments are disrupting economic and financial systems.** In particular, large technological companies (big techs) are rapidly scaling up the supply of products and services by taking advantage of their "data-network-activities" (DNA) loop.[4] This is progressively altering markets' structure and the competitive position of incumbents, including commercial banks.[5]

2. **The operations of big techs are expanding the available range of products and services.** Big techs provide financial services directly to consumers either in competition with traditional financial institutions or in partnership with them.[6] They also provide a range of services to financial intermediaries that facilitate consumer access to the products and services of financial institutions. Taken together, these services are expanding the range of products and services for consumers, often at lower costs and with enhanced customer experience, thereby improving customer outcomes and efficiency. Moreover, big techs in several jurisdictions are contributing to financial inclusion by expanding the availability of services, such as payments or credit underwriting, to segments of the population that were previously underserved or excluded from the market of financial services that was traditionally dominated by banks.[7]

3. **Yet the quick expansion of big techs is creating a number of challenges.** In particular, their DNA loop creates competitive dynamics that could easily lead to the concentration of different financial and non-financial services around a few technologically advanced players. That process may not only damage market contestability but also increase the vulnerability of the financial system (Carstens et al (2021)) by promoting a potentially excessive reliance of market players, including financial intermediaries, on the services offered by few providers.[8]

4. **Different jurisdictions are addressing the risks posed by big techs through various adjustments to the regulatory framework.** Especially, authorities are reviewing their regulatory perimeters or introducing new regulation in order to ensure that big tech activities are subject to sufficiently effective rules, aimed at protecting market integrity, consumer protection, data privacy and other policy goals.[9] Moreover, some jurisdictions are considering establishing specific laws and rules for big techs that could address the risks emerging from the combination of activities that they perform. This is particularly evident in the area of competition, where authorities are developing legislative initiatives aimed at fostering more players competing fairly in digital markets and constraining big tech practices in order to safeguard contestability.

5. **This paper reviews various regulatory initiatives developed in China, the European Union (EU) and the United States.** It is structured as follows. Section 2 briefly describes the typology of regulatory actions. Section 3 reviews recent initiatives in five different policy domains: competition, data, operational resilience, financial stability and conduct of business. Section 4 offers some concluding remarks.

[4] The business model of big techs is described in detail in BIS (2019); regulatory issues, challenges for public policy and policy options in Carstens (2018, 2021), Carstens et al (2021), Crisanto et al (2021), Restoy (2019, 2021a,b) and Shin (2019).

[5] See Feyen et al (2021) for a discussion of the implications of digital innovation for market structure and public policy.

[6] See Claessens et al (2018), Frost et al (2019) and Frost (2020) on the economic drivers of fintech/big tech activity across countries; and Cornelli et al (2020) on the size of fintech/big tech credit markets and the factors driving their growth.

[7] See Croxson et al (2021) and Frost et al (2021) for a discussion of the evidence to date.

[8] For example, Amazon Web Services (AWS) and Microsoft Azure dominate the public cloud market for financial services in Europe, the United States, the Middle East and Africa, according to 451 Research. Some 45% of financial services respondents to a 2019 market survey said they use AWS as their primary cloud provider, with a further 45% saying they use Microsoft Azure (Furber (2020)).

[9] See Ehrentraud et al (2020) for a cross-country overview of policy responses to fintech developments.

Section 2 – The different types of regulatory initiatives

6. **Big techs provide a relatively wide range of services.** Depending on the jurisdiction, these include e-commerce, social media, internet search and advertising, telecommunications, ride hailing, payment services, credit, wealth management and cloud computing services.[10] In jurisdictions where big techs may offer regulated financial services they must hold the required licence (eg as a payment institution or asset manager) and comply with the regulations established to conduct that activity. In addition, they are subject to cross-sectoral regulations such as those in the area of competition or data protection (Crisanto et al (2021)).

7. **Recent regulatory initiatives to address the risks posed by big techs can be roughly classified in two categories.** The first type of actions introduce adjustments to existing rules that indirectly affect big tech operations rather than introducing specific entity-based rules on big techs. In this category belong actions taken to improve personal data protection and data-sharing, or measures adopted to strengthen the operational resilience of firms with significant reliance on technology or third-party providers. Those initiatives typically follow an activity-based approach as they affect – albeit with different intensities depending on business models – all firms participating in one or several market segments.

8. **A second category includes initiatives that directly address the risks generated by big tech business models by imposing on them specific entity-based obligations and restrictions.** This approach aims at controlling the risks that emerge from the combination of activities that big techs perform as part of their unique DNA loop (BIS (2019); Restoy (2021a)). Examples of initiatives in this category are competition policies to prevent market abuse or data dominance. Other examples are rules imposed on big tech groups in order to protect their stability and resilience.

[10] For financial service offerings by big tech companies, see Table 1 in Crisanto et al (2021).

Section 3 – Relevant initiatives

9. **The extent of policy initiatives for big techs has expanded markedly over the last few years in several large jurisdictions.** China, the EU and the United States have already enacted or are currently considering actions in several policy areas, following their respective normative processes.[11] These areas are: (i) competition; (ii) data protection and data-sharing; (iii) conduct of business; (iv) operational resilience; and (v) financial stability. Each of the three jurisdictions has prioritised different areas. Given that big techs in China have a significant footprint in payments and financial services, authorities there have imposed stringent requirements in the area of financial stability. Regulators in the EU have developed wide-ranging frameworks on operational resilience, conduct of business and data protection. The boldest proposals currently considered in the US are in the competition domain.

10. **Policy initiatives need to be seen in their jurisdictional context.** In China, big techs have become significant or even dominant providers of financial services, most notably in payments but also in many other areas, and can therefore generate specific challenges for the preservation of financial stability. In the United States, there is a long-standing policy of separating commerce and finance.[12] This may in part explain why financial stability considerations have not been the focus of the normative actions undertaken so far in relation big techs. Relevant initiatives have rather primarily been geared towards preserving the contestability of markets. The EU, on the other hand, is a large market for big techs from outside Europe, and as such, overall efforts aim at controlling the perceived risks while reaping the benefits big techs bring to consumers and businesses. Moreover, how jurisdictions have prioritised policies, and the recent adjustments made, reflect not only the risks posed by evolutions in big tech activities but also perceived insufficiencies in the current regulatory framework.

11. **This section provides an overview of different regulatory initiatives in major jurisdictions.** It reviews recent initiatives in the policy areas highlighted above in China, the EU and the United States.

Competition and market contestability

12. **Competition policy is the area where regulatory initiatives have been most numerous and far-reaching.** The business model of big techs (through their DNA loop) creates opportunities to reach dominant positions in different market segments that can lead to excessive concentration and anticompetitive practices. In particular, big techs' market dominance can lead them to require exclusivity of participants, discriminate across potential or existing vendors, give preferential treatment to their own products, bundle their services, creating cross-product subsidisation, or abuse their wealth of data to gain a competitive advantage.[13]

13. **Up to now, competition authorities have generally followed a traditional approach to address anticompetitive behaviour of tech giants.** Big techs, like any other firm, are subject to general competition rules aimed at preventing collusive practices, abuse of market dominance or excessive market

[11] In China, legislation is adopted by the National People's Congress and its Standing Committee; administrative regulations are issued by the State Council and its subordinated administrative bodies, such as the State Administration for Market Regulation (SAMR), in their specific policy fields. In the EU, the European Commission – the only institution empowered to initiate legislation – proposes laws and, in most cases, the European Parliament and the Council co-legislate and jointly adopt legislation once they have reached consensus. In the United States, any member of Congress can propose legislation even with little support beyond the initiating member. Accordingly, proposed legislation should not be viewed as indicative of any future law, which both houses of Congress must pass and the president must approve before it can be enacted.

[12] See Box B in FSB (2019).

[13] In China, under current market practice, merchants are often restricted to the services that one big tech provides within its platform (a practice referred to as "pick one of two"). Users of one platform may not be able to easily access another platform's services, and customers may be quoted different prices generated by algorithms and face subsidised or inflated prices. See Box 3 in Restoy (2021a). For a discussion of antitrust concerns in the US, see eg Khan (2017).

concentration. Those general rules are enforced ex post by competition authorities which can reverse unlawful operations, require the suspension of specific business practices, ban mergers and acquisitions, and impose pecuniary sanctions. However, those actions typically need to be justified by sufficient evidence that firms' practices have a detrimental impact on consumer welfare.

14. **Some recent initiatives attempt to strengthen traditional ex post measures of competition policy.** They do so by enhancing the enforcement capacity of competition agencies, by increasing the intensity of competition enforcement and potential penalties for non-compliance (Box 1), and by lowering or reversing the burden of proof to evaluate mergers and acquisitions.[14]

15. **However, a paradigm shift is emerging with the development of ex ante entity-based rules.** To protect competition, these rules would constrain ex ante business practices of big techs.[15] This follows the realisation that the traditional ex post approach by competition authorities may prove ineffective to protect the interests of customers and prevent irreversible damage to market contestability, given the speed with which big techs can scale up their market penetration and distort competition (De la Mano and Padilla (2019)).

16. **Jurisdictions are moving to implement comprehensive ex ante competition requirements.** In general, ex ante requirements include ensuring the interoperability of online platforms with third parties, prohibiting restrictions for business users to deal with their customers or offer them products outside the platforms, and mandating equal treatment for all existing and potential business users in the platforms, including conditions for platforms not to give preference to their own competing products (in search results, rank etc) against those offered by business users.[16] Examples of initiatives introducing ex ante competition requirements in the three jurisdictions under review are the following (see Table 1):[17]

- In the US, the House of Representatives Subcommittee on Antitrust, Commercial and Administrative Law released a report in October 2020 investigating possible anticompetitive practices by big techs in their commercial activities and a series of recommendations to regulate them (US House (2020)). This report was followed by several legislative initiatives that are currently under discussion in the US Congress.[18] More recently, President Biden issued an Executive Order on Promoting Competition in the American economy, which mandates federal

[14] This would require entities to proactively justify that a prospective merger or acquisition does not create a risk of lessening competition. It also implies that enforcement actions would no longer require substantial proof that dominant firms' practices damage consumers' welfare if they are considered as anticompetitive by the authorities. See Senator Klobuchar's Competition and Antitrust Law Enforcement Act (CALERA), Senator Hawley's Trust Busting in the 21st Century Act and Representative Jeffries' Platform Competition and Opportunity Act of 2021.

[15] While these rules as proposed would apply to big techs, they may also apply to other large technology companies generally.

[16] Moreover, competition is also fostered by introducing specific requirements on data use and data-sharing obligations with third parties upon clients' consent (see Section 3.3).

[17] Recently, the UK government also issued a consultation paper setting out its proposals for a new "pro-competition regime for digital markets" (HM Government (2021)). The proposal would establish the Digital Markets Unit (DMU) in the Competition and Markets Authority (CMA), which would have powers to monitor and enforce the new regime. The DMU would be in charge of designating firms that have "strategic market status" (SMS), implementing a mandatory, enforceable code of conduct for these firms, and conducting "pro-competitive interventions" (eg data-related remedies and measures to enhance consumer choice) in cases where potential anticompetitive practices have been assessed. Both SMS designations and pro-competitive interventions are conducted with respect to a particular *activity* rather than a specific firm. However, any firms that have activities designated with SMS are also subject to enhanced merger and acquisition supervision, including enhanced reporting requirements and reduced thresholds for which authorities may intervene on a merger.

[18] Some of these initiatives include the ACCESS Act (H.R. 3849), Senator Klobuchar's CALERA, the Platform Competition and Opportunity Act (H.R. 3826), the American Choice and Innovation Online Act (H.R. 3816), and Senator Hawley's Trust Busting in the 21st Century Act, among others. See US House (2021a,b,c) and US Senate (2021a,b).

regulators across a variety of sectors to evaluate their competition frameworks and policies and propose new ones to regulate ex ante behaviours that are seen as anticompetitive.[19]

- In China, the State Administration for Market Regulation (SAMR) in February 2021 issued wide-ranging "Platform antimonopoly guidelines" specifying specific antitrust requirements for big tech companies.[20] Moreover, the People's Bank of China (PBC) issued for consultation specific pro-competition requirements in a new regulation for non-bank payment service providers in January 2021.[21]
- In the EU, the European Commission (EC) published in December 2020 its flagship legislative proposals for the Digital Services Act (DSA) and Digital Markets Act (DMA) to upgrade the rules governing digital services in the EU.[22] The DMA proposal lays down rules aiming at protecting contestability in those markets in which "gatekeepers" are present. This term is applied to large and systemic online platforms according to specific criteria covering geographical presence, total revenues, market capitalisation, number of active users etc. The DMA complements the enforcement of competition law at the EU and national levels, which will continue to apply fully and in parallel to any gatekeepers designated under the DMA.[23] As stated by the EC, the "Digital Markets Act addresses unfair practices by gatekeepers that either (i) fall outside the existing EU competition control rules, or, (ii) cannot always be effectively tackled by these rules because of the systemic nature of some behaviours, as well as the ex-post and case-by-case nature of competition law. The Digital Markets Act will thus minimise the harmful structural effects of these unfair practices ex-ante, without limiting the EU's ability to intervene ex-post via the enforcement of existing EU competition rules."[24]

[19] Broadly speaking, these initiatives include regulatory evaluations of competitive and concentration risks in key sectors of the US economy (eg healthcare, transportation, financial services), as well as specific tasks, such as limiting or banning non-compete clauses, strengthening consumer rights to repair equipment, and the facilitation of the portability of consumer financial transaction data. The Executive Order also advocates for more forceful ex post enforcement of antitrust laws by the Federal Trade Commission and Department of Justice.

[20] See SAMR (2021) for the guidelines (in Chinese); and Box 3 in Restoy (2021a) for an overview of recent changes in China's competition framework.

[21] For a translation, see PBC (2021).

[22] See EC (2020b,c). Further information about the legislative proposals can be accessed from the EC's webpages: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[23] One reason why the DMA introduces the distinct concepts of contestability and fairness could be the difficulty with establishing "dominance" and "abuses" in ex post competition cases. Because of this, the DMA is considered to operate outside existing competition law. As the EC makes clear in its communication, the DMA is without prejudice to the implementation of EU competition rules and to national competition rules regarding unilateral behaviour. See Digital Markets Act: Ensuring fair and open digital markets (europa.eu).

[24] See Digital Markets Act: Ensuring fair and open digital markets (europa.eu).

Key big tech competition guidelines and proposed legislation in selected jurisdictions Table 1

Jurisdiction	Regulation	Scope	Ex ante or ex post?		Instrument			
			EX A	EX P	BOP	INT	TPP	PRO
China	Platform Antimonopoly Guidelines	All online platforms. Additional provisions for "essential facilities", as well as provisions to identify potential abuses by dominant platforms.	✓	✓		✓	✓	✓
China	Regulation on non-bank payment service providers*	Non-bank institutions that provide payment services for natural persons, legal persons and other organisations.	✓	✓		***	***	***
EU	Digital Markets Act*	"Gatekeepers" with a strong, entrenched, and durable economic and intermediation position.	✓	✓**		✓	✓	✓
US	Competition and Antitrust Law Enforcement Act* (CALERA)	"Dominant" firms that have >50% of total market share or "significant" market power.	✓	✓	✓			
US	Augmenting Compatibility and Competition by Enabling Service Switching Act* (ACCESS Act)	Platforms that satisfy criteria for (i) monthly active users (individual or business); (ii) market capitalisation; and (iii) critical trading partner status.	✓	✓**		✓		
US	Platform Competition and Opportunity Act*	Identical scope as the ACCESS Act.	✓		✓			
US	American Choice and Innovation Online Act*	Identical scope as the ACCESS Act.	✓	✓**		✓	✓	✓
US	Trust Busting in the 21st Century Act*	Dominant platforms, determined by evaluating the (i) extent and durability of market power; (ii) government involvement (contracts etc), (iii) exclusivity agreements; (iv) network effects; and (v) vertical integration.	✓	✓**	✓		✓	
US	Bust up Big Tech Act*	Platforms that satisfy criteria for (i) yearly active users; and (ii) total revenue.	✓		✓		✓	

* Proposed.

** Ex post measures (eg fines) are specific to big techs.

*** If a non-bank payment institution meets certain conditions in terms of market share, the PBC may provide an early warning of measures it may take. Apart from regulatory interviews, these may include a range of measures to restore fair competition and a healthy development of the payment service market. The PBC can also advice the State Council's anti-monopoly law enforcement agencies to take measures against abuse of market dominance by requiring a breakup of the institution by separating different types of payment business.

BOP = shifting of the burden of proof from the regulator to the firm engaging in a merger or acquisition; INT = interoperability with third parties; PRO = allowing business users to promote and offer products and services and conclude contracts outside the platform; TPP = equal treatment of own and third-party products or services.

Source: Authors' compilation.

Box 1

Recent ex post supervisory and enforcement actions against big techs

Chinese authorities have engaged in a number of ex post supervisory actions against big techs. The initial public offering (IPO) of Ant Group rapidly unravelled after regulators blocked it for not complying with listing criteria and disclosure requirements. In April 2021, the group was forced to restructure and its affiliate, Alibaba, was fined RMB 18.23 billion ($2.8 billion) – the biggest antitrust fine levied in China to date. Additionally, regulators ordered 34 Chinese internet companies to undergo rectification of their business models for potential anticompetitive practices. A week later, the China Securities Regulatory Commission (CSRC) issued new rules aimed at restricting the listing of fintech and "model innovation enterprises" on the Shanghai Stock Exchange Science and Technology Innovation Board. Other large Chinese firms, such as Didi, Baidu, and Tencent, have also faced more intense scrutiny. Many penalties levied by Chinese regulators against these companies have been for past acquisitions and transactions, including those under "variable interest entity" structures.①

Supervisory authorities in the EU have imposed fines or initiated court proceedings against *individual firms* that may have violated anticompetitive rules. For example, since 2017 authorities have imposed three fines totalling €8.25 billion ($9.7 billion) on Google for anticompetitive behaviour. EU regulators are now investigating Google for favouring its own online display advertising technology services in the "ad tech" supply chain. Moreover, in 2020 EU regulators opened a series of investigations on possible anticompetitive practices by Amazon and Apple. The former is alleged to have made illegal use of non-public business data and to have favoured vendors using other Amazon services. The latter is being investigated for both its "gatekeeper" role in the distribution of apps and content to users, as well as its conduct regarding the use of its Apple Pay mobile payments solution.

In the United States, federal and state regulators have initiated actions against Google and Facebook for alleged anticompetitive behaviour. For Google, the supervisors' complaints centre around the company's dominance in search advertising markets, as well as practices to ensure that it is the default option on many smartphones, web browsers and devices such as smart TVs and speakers. The suits against Google are still pending. Facebook has received criticism due to its acquisitions of Instagram in 2012 and WhatsApp in 2014, which have prompted concerns that the company has substantial and entrenched market power. Separate lawsuits initiated by the Federal Trade Commission (FTC) and a group of state regulators were dismissed in June on the grounds that the burden of proof that Facebook had monopoly power as a result of the acquisitions was not met, and that the acquisitions had taken place some time ago. Finally, some proposed legislation that includes ex ante rules, such as CALERA, provides additional funding and resources to the FTC and Department of Justice; and establishes a new independent division at the FTC to conduct studies on market concentration and merger retrospectives, and provide recommendations on the competitive effects of government policies.

① Variable interest entities (VIEs), the prevailing structure for big techs, are offshore structures that allow Chinese companies to obtain foreign funding (eg in US dollars). In China, foreign investors are not allowed to own companies in key sectors; and setting up a VIE is a means of giving foreign shareholders access to the economic benefits of the underlying entity without them owning it or controlling its business. See eg www.ft.com/content/38ba7bb9-9a7e-4817-80cf-324bc9a4527b.

Data protection and data-sharing

17. **The use of consumer data is core to the business model of big techs.** These rely on a large number of users interacting in a digital ecosystem. This activity produces data that are then used as an input to offer products and services that generate further user activity and, in turn, more data (the DNA loop). Therefore, the ability to gain insights from users' data is a key competitive advantage for big techs. Regulatory constraints on this ability are important considerations for their business models.

18. **Several policy initiatives on data protection and data-sharing have taken form in the EU and China, and are under discussion in the US (Table 2)**. The European General Data Protection Regulation (GDPR) is one of the most influential pieces of legislation in both areas. Different legislative initiatives on data protection have also been put forward in the US (eg legislative proposals on the Consumer Online Privacy Rights Act (COPRA), the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE Data Act) and the United States Consumer Data Privacy Act (USCDPA)). In China, a new Data Security Law (DSL) and Personal Information Protection Law (PIPL) have been enacted. With respect to data sharing, the EU's second Payment Services Directive (PSD2) provides the core regulatory framework to release customer data in a secure environment. Last December's draft Digital Markets Act (DMA) seeks to reinforce the data portability rights included in GDPR[25], drawing on the experience acquired in the context of the implementation of the PSD2.

Data protection and data-sharing approaches in the EU, US and China — Table 2

	EU	US	China
Data protection			
Collection and use of personal data			
Of which: Lawfulness, fairness and transparency	√	√	√
Purpose specification	√	*	√
Security	√	√	√
Users' data rights			
Of which: Consent and access	√	*	√
Rectification and deletion	√	*	√
Data portability	√	*	√
Data-sharing			
Open banking			
*Approach: prescriptive, facilitative**, market-driven****	Prescriptive	Market	Market

Legend: Comprehensive | Partial | Early stages

* While there is no federal law addressing these elements at present, they are subject to ongoing debate.

** Under a facilitative approach, jurisdictions issue guidance and recommended standards, and release open API standards and technical specifications.

*** No explicit rules or guidance that either require banks or prohibit them to share customer-permissioned data with third parties.

Sources: BCBS (2019) and authors' compilation.

[25] See DMA Article 6, in particular Articles 6(1)(a) and 6(1)(h).

19. **Proposed data protection frameworks in the US and the finalised framework in China show a high degree of alignment with the EU's GDPR.** This is particularly the case with respect to data processing expectations and users' data protection rights. In the area of data processing, all these frameworks include similar expectations related to the collection and use of personal data (ie fairness, lawfulness, transparency and accuracy). Especially relevant for big techs is the emphasis that these frameworks put on "purpose specificity" and security requirements. The former calls for users' data to be collected and utilised for the purpose consented by the respective user. The latter alludes to technical and organisational measures to protect the integrity, confidentiality and availability of users' data.

20. **These frameworks also share many of the main features related to users' data rights.** The underlying principle behind them is that individuals have distinct or defined rights with regard to personal data. As such, laws in the EU and China not only require users' consent to process their data but also entitle users to access, rectify and delete their information. A key component of data protection frameworks relevant for big tech business models is the ability to transfer personal data across borders. The general approach in the EU and China is that these transfers can take place only if authorised by the competent authority or if appropriate levels of protection are in place.[26]

21. **Another important feature is the right to data portability.** This right entitles users to get their personal data back so that they can use it for their own purposes, or to ask for their personal data to be transferred to third parties in a technically feasible format. In the EU, the GDPR requires all firms to share clients' data with third parties at the customers' request. As such, it adds strength to open banking provisions under PSD2 by creating consistent expectations across third parties. However, GDPR applies only to the data of natural persons and not to those of firms, and it lacks a technical standard for the transmission of information.

22. **Developments in data portability and data-sharing are paving the way for comprehensive adoption of open banking.**[27] Both the GDPR and PSD2 create portability rights in the EU. PSD2 requires banks, e-money and other payment institutions to share their clients' payment account information upon their consent with licensed third parties that provide payment initiation and account information services (both of which are provided by big techs[28]). To operationalise this arrangement, PSD2 requires obliged entities to set up a standardised access interface to clients' accounts such as application programming interfaces (APIs) and strict security requirements such as strong customer authentication (SCA).[29] In comparison with the prescriptive approach to open banking in the EU, the US and China seem to be following a market-driven approach (Table 2).

23. **Pivoting towards a (broader) open banking framework in the EU would require additional measures.** In its October 2020 Digital Finance Strategy,[30] the EC announced that it will present a legislative proposal for a new open finance framework by mid-2022, building on and in full alignment with broader data access initiatives, including the proposals for the DMA and DSA. In this regard, the proposed DMA is envisaged to bring more symmetry to the European data-sharing regime by requiring the "gatekeepers"

[26] In the case of the GDPR, "appropriate levels of protection" include situations in which the EC has decided that a third country ensures an adequate level of data protection or, alternatively, this is ensured through legally binding agreements. Although the approach is similar in China, the recent PIPL and the DSL require companies to obtain the approval of a yet-to-be-identified office of the government before providing data to non-Chinese judicial or law enforcement entities.

[27] Open banking can be defined as a collaborative model in which bank customers have the right to transmit their data in digital form (generally through APIs) and hence are entitled to use online services of different banks and non-bank financial service providers in a secure and convenient manner.

[28] Following the PSD2's entry into force, big techs such as Alipay, Facebook and Amazon obtained their e-money authorisation. Amazon is also authorised to operate under this framework, but its e-money licence was obtained under PSD1 (see EBA's register of payment and electronic money institutions under PSD2, www.eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2).

[29] See EBA (2017).

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591.

to provide effective portability of data generated through users' activity. Under this provision, payment institutions could obtain data from big techs and use them – upon clients' consent – for their own business purposes.

24. **Regulatory developments in China are expected to have far-reaching implications for how big techs collect, use and manage their customer data.** The PIPL, which is arguably modelled on the GDPR and will enter into force on 1 November 2021, seeks to protect personal information rights and interests, regulate the processing of personal information and promote the reasonable use of personal information (Article 1).[31] This new law specifies the conditions under which personal data can be collected, including obtaining an individual's consent, and grants individuals various rights to their personal information, including the right to data portability.[32] Moreover, it imposes additional obligations on big techs that require them, for example, to set up a compliance system for personal information protection; establish an independent body composed mainly of external members to protect personal information; and regularly release social responsibility reports regarding personal information protection.[33] PIPL complements China's new DSL, which came into effect on 1 September 2021 and contains provisions that cover the usage, collection and protection of data, with a view to safeguarding national security.[34] In that context, a debate has emerged on trade-offs and limits of alternative information arrangements between big techs and banks (Gambacorta et al (2021)).[35]

25. **In the United States, data privacy is generally regulated at the state level.** The most ambitious data privacy legislation at the state level is the California Consumer Privacy Act (CCPA), which requires that data subjects be informed about when and how data are collected and gives them the ability to access, correct and delete such information.[36] The CCPA also recognises a right to data portability, which requires businesses to provide data "in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance".[37] In New York, a bill (the NY Privacy Act) is currently under consideration that aims to "address how online platform/social media firms process personal data."[38] It also includes a right to data portability.[39]

26. **The Biden administration is encouraging rulemaking on portability of consumer financial data.** President Biden's July 2021 Executive Order encourages the Consumer Financial Protection Bureau

[31] On data use, PIPL imposes restrictions on the transfer of data from one personal information processor to another, which may only take place if certain conditions are met. See PIPL Articles 21–23. A translation into English can be accessed at www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation.

[32] Article 45 stipulates that when data subjects request a transfer of their personal information to other Data Controllers that they designate, and such requests conform with the conditions set by the State Cyberspace Administration, the Data Controller shall provide the methods for the transfer. See www.jdsupra.com/legalnews/personal-information-protection-law-4689872/.

[33] Article 58 puts additional obligations on "personal information processors that provide important internet platform services with a large number of users and complex business types shall perform the following obligations".

[34] See www.cma.gov.cn/2011xwzx/2011xmtjj/202106/t20210611_578547.html.

[35] In China, one option is to establish a separate credit scoring entity that is partly state-owned (Yu and McMorrow (2021)).

[36] The California Privacy Rights Act (CPRA), which is amending and expanding the CCPA, will take full effect in 2023. Other states that have enacted privacy laws include Virginia (Consumer Data Protection Act) and Colorado (Colorado Privacy Act). In some states, legislative initiatives with a narrower scope have emerged. In Massachusetts, for example, a ballot initiative was passed "to provide motor vehicle owners and independent repair facilities with expanded access to wirelessly transmitted mechanical data related to their vehicles' maintenance and repair". See www.sec.state.ma.us/ele/elepdf/IFV_2020.pdf.

[37] CCPA Section 1798.100.

[38] The NY Privacy Act would require "the companies to attain consent from consumers before they share and/or sell their information by acting as fiduciary entities". See www.nysenate.gov/legislation/bills/2019/s5642.

[39] In September 2020, the FTC held a workshop to examine the potential benefits and challenges to consumers and competition raised by data portability. See www.ftc.gov/news-events/events-calendar/data-go-ftc-workshop-data-portability.

(CFPB)[40] to issue rules "under section 1033 of the Dodd-Frank Act to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products" (White House (2021)). In July 2018, the US Treasury issued a report[41] that recommended the development of regulatory approaches to enable secure data-sharing in financial services (US Treasury (2018)). In the meantime, major US banks have been developing API-based offerings, in contractual partnerships with third parties, as a way to attract new customers and maintain/gain competitive advantage.[42] On the part of tech companies, Apple, Facebook, Google, Microsoft and Twitter are working on their Data Transfer Project with the goal of creating an "open-source, service-to-service data portability platform so that all individuals across the web could easily move their data between online service providers whenever they want".[43]

Conduct of business

27. **Big techs, by definition, serve a myriad of customers, in some cases over 2 billion each month.**[44] Thus, it is not surprising that the relationship between a big tech platform and its users – how they are treated and what information they receive – is a matter of public concern. Policymakers may therefore seek to bring balance into this relationship by introducing safeguards that ensure big techs treat their customers fairly and provide them with information that allows them to assess whether a particular service is suitable for them, and whether they are content with their end of the bargain, including how their data are being used and possibly monetised.

28. **Up to now, there have not been any comprehensive efforts to address potential conduct issues of big tech firms.** Perhaps the most notable development in this area is the EU's proposed DSA, which aims "to set out uniform rules for a safe, predictable and trusted online environment"[45] where fundamental rights enshrined in the Charter of Fundamental Rights of the European Union are effectively protected.[46] To create this protection, the DSA establishes a transparency and accountability framework for online platforms and sets out requirements (i) to prevent platforms from being misused to spread illegal content such as hate speech, or to offer illegal services; and (ii) to change current practice under which online platforms may delete users' content, without informing them or providing a possibility of redress.[47]

29. **In the EU DSA, entities classified as "very large online platforms" face the most extensive requirements.**[48] These include the obligation to conduct risk assessments on what the draft DSA calls "systemic risks stemming from the functioning and use made of their services". Under the draft DSA,

[40] In 2017, the CFPB released a set of non-binding Consumer Protection Principles on consumer-authorised financial data-sharing and aggregation. See https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[41] US Treasury (2018).

[42] See www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-around-the-world.html.

[43] https://datatransferproject.dev/.

[44] Facebook, for example, has over 2 billion monthly active users (IBFED and Oliver Wyman (2020)).

[45] Draft DSA, Recital 3 and Article 2.

[46] The DSA would complement the DMA, which also seeks to enhance protections for end users.

[47] See https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment/europe-fit-digital-age-new-online-rules-users_en.

[48] Very large platforms are defined as online platforms which provide their services to 45 million or more average monthly active recipients in the EU (Article 25). The Digital Services Coordinator of establishment shall verify, at least every six months, whether any platform in its jurisdiction meets the criteria. In that case, it shall adopt a decision designating the online platform as a very large online platform for the purposes of the DSA, or terminate that designation. The EC shall ensure that the list of designated very large online platforms is published in the Official Journal of the European Union and keep that list updated.

systemic risks are defined to include the risk of a very large online platform (i) being misused to disseminate illegal content and amplify access to such content through accounts with a particularly wide reach; (ii) to infringe on the fundamental rights protected by the Charter of Fundamental Rights, including the freedom of expression and information, the right to private life and the right to non-discrimination; and (iii) being intentionally manipulated "with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, [...] electoral processes and public security", eg through the creation of fake accounts and the use of bots.[49]

30. **Once enacted, the draft DSA will complement existing regulation that governs the relationship between digital platforms and their business users.** As regards professional users of online platforms, the DSA would complement and expand existing transparency and fairness rules in the EU under its *Regulation on promoting fairness and transparency for business users of online intermediation services* (P2BR), which entered into force in July 2020 and focuses on procedural fairness in the relationships between platforms and their business users. P2BR obliges all online platforms, regardless of size, to be transparent on key issues such as ranking, possible self-preferencing and data access, to notify professional users of contractual changes and account delisting, and to offer redress possibilities.[50]

31. **Outside the EU, while most legislative initiatives on big tech focus on policy areas other than business conduct, a few are aimed at protecting consumers.** As one example, for e-commerce in China, the SAMR issued rules on online transactions in March 2021 to "protect the legitimate rights and interests of online consumers"[51] by offering protection against online merchants following deceptive or misleading practices, such as fake transactions and user reviews, and false marketing.[52]

Operational resilience

32. **The EU and China have taken regulatory action on operational resilience.** Their initiatives are centred on rules and requirements to: (i) ensure that all sources of operational risk for financial institutions are identified and evaluated; (ii) ensure the continuity of information and communications technology (ICT) services; and (iii) facilitate a swift response in the event that services are disrupted. These requirements may be incorporated into an activity-based initiative, as is the case with the proposed Digital Operational Resilience Act (DORA) in the EU,[53] or be part of an entity-based framework, as they are in China's regime for financial holding companies.

33. **The EU's DORA is the most comprehensive framework to date on digital operational resilience in the financial sector.** The Act seeks to harmonise digital operational resilience requirements across the EU financial sector, including by imposing requirements on the security of network and information systems for all entities involved in the provision of financial services, including credit institutions, audit firms, insurance intermediaries, credit rating agencies and ICT third-party service providers. The Act would mandate all financial institutions to create an ICT risk management framework that must be evaluated and tested yearly. In addition, all firms must have a "crisis management function" in charge of communications if an ICT breach occurs, follow technical standards for incident-related reporting requirements and manage third-party ICT risk.

[49] Draft DSA, Recital 57 and Article 26.

[50] For a summary, see Busch (2020).

[51] Global Times (2021b).

[52] In the EU, rules with similar objectives have been in established in 2002 under the Directive on Distance Marketing of Financial Services (DMFSD), which aims to protect consumers when they sign a contract with a retail financial services provider at a distance (eg via phone or online). The DMFSD is currently under review. See https://data.consilium.europa.eu/doc/document/ST-12646-2020-INIT/en/pdf.

[53] See EC (2020a) and https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.

34. **The DORA proposal discusses requirements for the management of third-party ICT service providers and establishes an oversight framework for those designated by the EC as "critical".** For these providers, an EU-level oversight and assessment framework – led by a Lead Overseer – would be established.[54] The Lead Overseer would be responsible for conducting assessments of these providers and subjecting them to additional, more stringent requirements based on the results of the assessment. Thus, the DORA proposal seeks "to address the lack of appropriate oversight powers to monitor risks stemming from ICT third-party service providers, including concentration and contagion risks for the EU financial sector."[55]

35. **For big techs, DORA is relevant in two ways.** First, big techs as *users* of third-party services in their financial services operations would have to abide by technical standards on evaluating and monitoring third-party risk, including the development of minimally disruptive exit strategies if a third-party provider is compromised.[56] Since big techs in the EU either directly conduct financial services as payments or e-money institutions, or do so in partnership with third-party organisations, DORA will be relevant for them. Second, big techs as *providers* of third-party services that are considered "critical" (eg cloud computing) will become subject to additional requirements and direct supervision by the Lead Overseer. The Lead Overseer will be able to solicit all documentation it may deem necessary for supervision, conduct general investigations on the third-party ICT provider and impose penalties on critical third-party ICT providers that are found in violation.

36. **In China, ensuring operational resilience is part of the PBC's regime for financial holding companies (FHCs).** The FHC framework includes some entity-based operational resilience requirements that affect the entire group, though these are less detailed than the ones proposed in DORA. The regime requires all FHCs to establish a comprehensive risk management system based on both qualitative and quantitative methods that will monitor various risks, including operational, and IT risks. The FHC framework also includes risk isolation mechanisms for all entities in the group that should, among other things, take account of the sharing of IT systems, supporting operating systems, business facilities and business premises.

37. **In the United States, federal banking agencies have oversight powers to monitor big techs as significant third-party service providers to banks.** Through the significant Service Provider Program established under the Bank Services Company Act, they have devoted substantial resources to overseeing big tech companies as service providers to banks. One focus of this oversight is operational resilience.[57]

Financial stability

38. **There have been comparatively fewer initiatives primarily aimed at mitigating potential systemic implications of big tech financial activities.** China has adopted the most initiatives in the area of financial stability. For example, the PBC adopted two significant measures affecting non-bank payment service providers, particularly big techs. First, in January 2019 it instituted a 100% reserve requirement for

[54] Designation criteria include size, substitutability with other providers, impact that the failure of the third-party provider would have on the quality or continuity of the provision of financial services in the EU, and reliance on the third-party provider in relation to the provision of critical or important functions that ultimately involve the same provider.

[55] See page 3 of the DORA proposal.

[56] Big techs' heavy reliance on technology services – either developed in-house or contracted out to third parties – represents a substantial source of operational risk that would need to be accounted for under DORA.

[57] In addition, in July 2021 the agencies issued for consultation a proposed interagency guidance on managing risks associated with third-party relationships. The guidance, which would be directed to all banking organisations supervised by the Federal Reserve Board, Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, outlines risk management principles for the different stages in the life cycle of third-party relationships, and sets forth considerations with respect to the management of risks arising from these relationships. See www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.

customer balances in big techs' payments accounts ("float") and required them to deposit the float in a reserve account with the PBC.[58] Second, in January 2021 it announced new rules for the deposit, use and transfer of customer reserves, applicable to non-bank payment institutions.[59] Under the new rules, payment companies and platforms need to deposit customers' money reserved for payment transactions to a designated bank account at the PBC, and to settle payment transactions only via the PBC account. A key effect of these rules is that big techs – which make up the majority of payments activity China – will not be able to engage in the business of risk transformation (ie granting credit, investing in interest-bearing assets) because all funds will need to be kept at the PBC.

39. **Chinese regulators have issued new requirements for online lending, which aim to alter the relationship of banks with big techs.** The considerable increase in online loans originated by bank-fintech partnerships in China prompted the Chinese Banking and Insurance Regulatory Commission (CBIRC) to release new guidelines for firms seeking to issue these loans. The CBIRC's guidance: (i) requires banks to jointly contribute funds to any online loans made with a partner; (ii) designates a minimum limit for a partner institution's contribution to the loan; and (iii) imposes an individual and total cap on the amount of the loans that banks are allowed to have with non-bank lenders.[60]

40. **A more far-reaching approach has been the creation of a specific regime for FHCs which directly affects big techs.** The PBC, which supervises all FHCs, requires all firms that hold two or more different types of financial services companies (eg commercial banks, trust companies) that exceed certain size thresholds to create FHCs under the new guidance.[61] The PBC's rules impose new rules on corporate governance, company structure, shareholder eligibility, related transactions and capital adequacy, among other requirements (Box 2). CITIC Group and China Everbright Group have already submitted FHC applications to the PBC, and both Tencent and Ant Group have been tapped by the PBC to submit their own applications by the deadline of 1 November 2021.

41. **Unlike some of the previous areas of focus, there has not been any direct action in the EU and US to specifically address potential financial stability risks associated with big techs.** This may be due in part to the fact that big techs have a comparatively smaller influence in financial services in those jurisdictions than in China, where they are mainstays of the payments and lending ecosystems. One notable development recently, however, was the EC's Call for Advice. In February 2021, the EC issued a request to the European Supervisory Authorities (ESAs) to provide an assessment of the existing supervisory perimeter to determine if any changes should be made to better capture the risks arising from the increased involvement of platforms and technology firms (including "techno-financial" conglomerates) in financial services.[62] Furthermore, the request, which highlights that new proposals – such as DORA – do not directly address the *prudential* risks that big techs in financial services may carry, expressly requires the ESAs to consider in their assessments the role of big techs in financial services. The European Banking Authority (EBA) has recently issued a report that calls for deepening the understanding of financial, operational and reputational interdependencies between financial institutions and technology companies outside the competent authorities' perimeter of direct supervision (EBA (2021)). The ESAs are expected to provide their joint assessment by January 2022.

58 See Box III.C in BIS (2019).

59 Global Times (2021a).

60 Partner institutions must contribute at least 30% of the funding for any loan issued jointly with a commercial bank. The balance of internet loans issued by a bank through any single platform cannot exceed 25% of the bank's Tier 1 capital. The total balance of internet loans issued jointly by a bank with all its online partners cannot exceed 50% of total outstanding loans.

61 For a translation of the FHC rules, see PBC (2020).

62 For a discussion on big techs as the next generation of financial conglomerates and the implications for supervision, see Noble (2020).

Box 2

Licensing of financial holding companies (FHCs) in China

On 11 September 2020, the PBC passed its *Trial Measures on Regulation of Financial Holding Companies* ("the Measures"), a comprehensive entity-based framework to enhance the regulation of large non-financial companies that have significant interests in financial services. Companies that control two or more different types of financial companies, which could be commercial banks, trusts, financial asset managers, securities companies, public fund management companies, futures companies or insurers or insurance asset management companies, are required to apply. Additionally, these financial companies must exceed certain size thresholds:

(1) if the company controls a commercial bank with total assets exceeding RMB 500 billion, or if the total assets of the commercial bank are less than RMB 500 billion, the total assets of other types of financial institutions exceed RMB 100 billion, or the total client assets exceed RMB 500 billion;

(2) if the company does not control a commercial bank and the total assets of the other types of financial institutions exceed RMB 100 billion, or the total client assets exceed RMB 500 billion; or

(3) if the company does not meet either of the two criteria above but the PBC deems it necessary to form an FHC for "macroprudential regulatory requirements".

FHCs under this regulation may not conduct non-financial business unless their non-financial assets are kept to no more than 15% of total assets. FHCs are subject to capital requirements at the level of the holding company and the financial subsidiaries and must establish a capital replenishment mechanism to support them. Additionally, they must establish "risk disposal" plans in the event that the FHC or its subsidiaries become distressed such that financial stability is threatened. If the FHC is unable to resume normal operation to the satisfaction of the PBC it may be required to adopt certain "bail-in" measures for additional capital relief. FHCs also face hard caps on intragroup transactions (guarantees or financing) which cannot exceed 10% of the net capital of the FHC or 20% of the net capital of the affiliate institution, as well as prohibitions on other related transactions.

There are a number of governance provisions as well. A controlling shareholder of a FHC must retain its controlling interest for at least five years and is subject to additional requirements about its relationships with related parties, potential abuse of market power or technological dominance, and market manipulation. Controlling shareholders must also be in good financial condition and have made a profit for each of the last three years. The Measures also require that the ownership structure of the FHC, as well as the financial institutions it controls, be simple, clear and transparent, with a maximum of three corporate levels. To help mitigate conflicts of interest, independent directors can serve a maximum of six years, and cannot own more than a combined 1% of the FHC and any subsidiaries under it. Non-independent directors can hold a combined maximum of 5%.

Section 4 – Concluding remarks

42. **Policymakers are taking action on big techs.** Several regulatory initiatives have been taken recently in China, the EU and the United States to address new challenges presented by big techs, specifically in the areas of competition, data, conduct of business, operational resilience and financial stability. While each of these jurisdictions places emphasis on different policy areas – and consequently policy objectives – the widest range of initiatives have been conducted in the area of competition. While several regulatory initiatives under consideration are mainly activity-based, authorities are progressively developing entity-based rules to address the unique combination of risks posed by these firms.

43. **All in all, recent initiatives in China, the EU and the United States represent important steps in combating relevant risks posed by big techs.** It seems likely at this stage that new policy developments may need to introduce further specific controls for big techs if they continue, as expected, gaining presence in the financial system either directly or through their engagement with financial institutions. It is also likely that, in order to address the risks that big techs generate through their unique (DNA loop) business models, those new policy actions will largely follow an entity-based approach and require close cooperation between competition, data and financial authorities.

44. **There is already a compelling case to seek international consistency of policy developments.** Given the cross-border scope of the activities performed by big techs, international regulatory cooperation seems essential. Several proposals have been put forward for enhancing the global collaboration on the design of policies aiming at addressing the challenges posed by digital technologies.[63] There have also been efforts by international standard-setting bodies to ensure that existing financial regulation (particularly in the area of payments) properly covers the activity of new non-bank players. As the need for specific rules for big techs may gain ground in different jurisdictions, the availability of common international guidance on the matter should help contain the risk of regulatory fragmentation.

[63] For instance, Ravi Menon, Managing Director of the Monetary Authority of Singapore, calls for remaking the world that was forged after Bretton Woods and for setting the rules of the game for international digital flows and international e-commerce (www.mas.gov.sg/news/speeches/2020/resilience-in-crisis-trends-beyond-covid19); the Centre for International Governance Innovation proposes the creation of a Digital Stability Board (www.thescienceofwheremagazine.it/2021/02/01/towards-the-digital-stability-board-for-a-digital-bretton-woods/); and Mastercard and other global companies suggest the establishment of a G7 Data and Technology Forum (www.mastercard.com/news/research-reports/2021/setting-principles-for-the-digital-economy-establishing-a-g7-data-and-technology-forum/).

References

Bank for International Settlements (2019): "Big tech in finance: opportunities and risks", *Annual Economic Report*, Chapter III, June.

Basel Committee on Banking Supervision (BCBS) (2019): *Report on open banking and application programming interfaces*, November.

Busch, C (2020): "The P2B Regulation (EU) 2019/1150: Towards a 'Procedural Turn' in EU Platform Regulation?", *Journal of European Consumer and Market Law*, vol 133, August.

Carstens, A (2018): "Big tech in finance and new challenges for public policy", keynote address at the FT Banking Summit, 4 December.

——— (2021): "Public policy for big techs in finance", introductory remarks at the Asia School of Business Conversations on Central Banking webinar, "Finance as information", Basel, 21 January.

Carstens, A, S Claessens, F Restoy and H S Shin (2021): "Regulating big techs in finance", *BIS Bulletin*, no 45, August.

Claessens, S, J Frost, G Turner and F Zhu (2018): "Fintech credit markets around the world: size, drivers and policy issues", BIS Quarterly Review, September.

Cornelli, G, J Frost, L Gambacorta, R Rau, R Wardrop and T Ziegler (2020): "Fintech and big tech credit: a new database", *BIS Working Papers*, no 887, September.

Crisanto, J C, J Ehrentraud and M Fabian (2021): "Big techs in finance: regulatory approaches and policy options", *FSI Briefs*, no 12, March.

Croxson, K, J Frost, L Gambacorta and T Valletti (2021): "Platform-based business models and financial inclusion", BIS Paper, forthcoming.

De la Mano, M and J Padilla (2019): "Big tech banking", *Journal of Competition Law & Economics*, vol 14, issue 4, April.

Ehrentraud, J, D Garcia Ocampo, L Garzoni and M Piccolo (2020): "Policy responses to fintech: a cross-country overview", *FSI Insights on policy implementation*, no 23, January.

European Banking Authority (2017): *Final draft Regulatory Technical Standards on strong customer authentication and secure communication under PSD2*, 23 February.

——— (2021): Report on the use of digital platforms in the EU banking and payments sector, September.

European Commission (2020a): Proposal for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, 24 September.

——— (2020b): Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 2000/31/EC, 15 December.

——— (2020c): Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 15 December.

Feyen, E, J Frost, L Gambacorta, H Natarajan and M Saal (2021): "Fintech and the digital transformation of financial services", *BIS Papers*, no 117, July.

Financial Stability Board (FSB) (2019): *BigTech in finance: market developments and potential financial stability implications*, December.

Frost, J (2020): "The economic forces driving fintech adoption across countries", *BIS Working Papers*, no 838, February.

Frost, J, L Gambacorta, Y Huang, H S Shin and P Zbiden (2019): "Big tech and the changing structure of financial intermediation"; *Economic Policy*, vol 34, no 100, pp 761–99.

Frost, J, L Gambacorta and H S Shin (2021): "From financial innovation to inclusion", *Finance & Development*, Spring.

Furber, S (2020): "As 'big tech' dominates cloud use for banks, regulators may need to get tougher", 18 August.

Gambacorta, L, F Khalil and B Parigi (2021): "Big Techs vs Banks", *BIS Working Papers*, forthcoming.

Global Times (2021a): "China announces customer reserves management measure for non-bank payment institutions", 23 January.

——— (2021b): "New rules on online transactions unveiled at China's annual Consumer Rights Day gala", 16 March.

HM Government (2021): "A new pro-competition regime for digital markets", July.

International Banking Federation (IBF) and Oliver Wyman (2020): *Big banks, bigger techs? How policymakers could respond to a probable discontinuity,* July.

Khan, L (2017): "Amazon's antitrust paradox", *The Yale Law Journal*, vol 26, no 3, January.

Noble, E (2020): "The next generation of financial conglomerates: BigTech and beyond", *Butterworths Journal of International Banking and Financial Law,* September.

People's Bank of China (2020): Order No. 4 [2020] of the People's Bank of China – Trial measures on regulation of financial holding companies*,* 11 September.

——— (2021): "Regulations on non-bank payment institutions (draft for comments)", 21 January.

Restoy, F (2019): "Regulating fintech: what is going on and where are the challenges?", speech at the ASBA-BID-FELABAN XVI Banking public-private sector regional policy dialogue on "Challenges and opportunities in the new financial ecosystem", Washington DC, 16 October.

——— (2021a): "Fintech regulation: how to achieve a level playing field", *FSI Occasional Papers*, no 17, February.

——— (2021b): "Regulating fintech: is an activity-based approach the solution?", speech to the fintech working group at the European Parliament, 16 June.

Shin, H S (2019): "Big tech in finance: opportunities and risks", speech on the occasion of the BIS Annual General Meeting, June.

State Administration for Market Regulation (2021): Antitrust Guidelines of the Antimonopoly Committee of the State Council on the Economic Field of Platforms, 7 February.

US House of Representatives (2020): Investigation of Competition in Digital Markets – Majority Staff Report and Recommendations, House Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary, October.

——— (2021a): H.R. 3849 – Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, 11 June.

——— (2021b): H.R. 3816 – American Choice and Innovation Online Act, 23 June.

——— (2021c): H.R. 3863 – Platform Competition and Opportunity Act of 2021, 24 June.

US Senate (2021a): Competition and Antitrust Law Enforcement Reform Act, 4 February.

——— (2021b): Trust-busting in the Twenty-First Century Act, 12 April.

US Treasury (2018): *A financial system that creates economic opportunities – nonbank financial, fintech, and innovation*, July.

White House (2021): Executive Order on Promoting Competition in the American Economy, 9 July.

Yu, S and R McMorrow (2021): "Beijing to break up Ant's Alipay and force creation of separate loans app", Financial Times, 13 September.