WINTER 2021 / ISSUE NO.18

$ 15.00 | € 10.00 | 1500 RSD

HORIZONS

ISSN 2406-0402

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

THE (NOT SO) ROARING TWENTIES?

BREMMER • ČIČAK • DORSEY • FRIEDMAN • GENSER • GRLIĆ RADMAN
HERRMANN • KHAN • KHANNA • LANDSMAN • LO • MA
MINUTO-RIZZO • MYERSON • PETERSEN • RUDD • TROITSKIY • YUSTE

cirsd.org

Breaking the Big Tech Monopoly

The Coming Decade of Big Tech Regulations

Winston Ma

FOR Chinese internet giants, 2020 started as a year of tremendous growth. Amid a pandemic crisis, tech giants demonstrated better real-time data of people's new daily routines, modified spending patterns, and their travel destinations (or lack thereof) than the government itself. Their mobile services have more reliable users' location data. Their digital payment systems record people's money spending habits and to whom they send money. Their apps also know what train, airplane, or concert tickets users have just bought. None of these things could be easily managed even by the most joined-up of bureaucracies, coordinating across agencies and ministries. In the end, many government efforts were hosted by internet platforms like Alibaba and Tencent to take advantage of their exiting user networks—which grew further over the course of the year.

Building on the momentum, Ant Group, the fintech arm of Alibaba, planned to launch a mega IPO in November 2020. The dual listing in Shanghai and Hong Kong, which had sought to raise $34.5 billion and would have valued Ant at over $313 billion, was expected to break the IPO-proceedings record set by Saudi Aramco, the state-owned oil giant of Saudi Arabia. As the largest online platform in China (and the world) for mobile payments and personal loans, the financial-services company received over $3 trillion in orders from retail investors across its dual listings.

***Winston Ma**, an Adjunct Professor at the NYU School of Law, is a former Managing Director and Head of the North America office of the China Investment Corporation (CIC), China's sovereign wealth fund. Prior to that, he served as the deputy head of equity capital markets at Barclays Capital, was a vice president at J.P. Morgan investment banking, and served as a corporate lawyer at Davis Polk & Wardwell LLP in New York. He is the author of several books, including* Investing in China *(2006),* China's Mobile Economy *(2016),* The Hunt for Unicorns *(2020), and* The Digital War *(2021). You may follow him on Twitter @Winston_W_Ma.*

Yet less than 48 hours before it was due to go public, Ant halted its planned Shanghai and Hong Kong listings as Chinese regulators published new draft rules for online lending. Meanwhile, the market saw a consultation draft of the Anti-Monopoly Guidelines on the "sector of platform economies" from antitrust agencies. In the same month, the central government also released the first draft of its comprehensive Law on Personal Data Protection, expected to become effective later in 2021, which restricts internet platforms' ability to collect and use consumer data. Within weeks, China's state watchdogs conducted regulatory talks with Ant Group, but also fined the company in parallel to launching an antitrust investigation into Alibaba. In March 2021, the *Wall Street Journal* reported that China's "antitrust regulators are considering levying a record fine against Alibaba." As a consequence of all this, Ant Group's IPO has not yet resumed as of March 2021.

> *Although geopolitical tensions are ever-present in the emerging post-pandemic world, all the major powers seem to share a consensus on at least one important issue, namely that Big Tech firms (irrespective of where they may be headquartered) are too big, too powerful, and too profitable.*

Taken together, these actions mark the first time the Chinese government has directly and systematically tackled anti-competitive behavior in the internet sector. It appears that the Chinese government has decided to be more active in taking steps to curb high-flying digital platforms' power and dominance in the country. This signals the end of an era, as the rising regulations will fundamentally change the competition landscape in China for internet companies.

China's latest actions also fit within an increasing global trend of regulators taking action against major internet platforms—what are called the "Big Tech" firms. Regulators from around the world are intensifying their scrutiny of Big Tech and reining-in their potential anti-competitive practices. In the European Union, for example, Facebook was levied with a record $5 billion fine in 2019 for violating consumer privacy rights, and Amazon was charged for antitrust concerns. Google was fined over $9 billion in antitrust penalties by the EU, and three antitrust lawsuits were brought against it in the United States in just a two-month period at the end of 2020.

No doubt, at the beginning of this new decade, the world is waking up to the reality that tech businesses also have a dark side, like other leading

companies in other industries. With nearly one billion internet users, China has the largest internet population—more than the U.S. and India combined. Thus, it provides the best context and case study for the regulation of Big Tech firms. This essay will examine the reasons behind China's development of a legal framework to restrain the power of Big Tech, how Chinese actions could be a catalyst for a global regulatory drive of Big Tech companies (especially in the United States), and what global collaboration is needed for what is arguably one of the most important policy initiatives in the coming decade.

THE AGE OF AI

Let us first go back in time. For China, the years of 2014-2015 have come to be seen as the most important inflection point in the history of the internet, as the country's internet population officially entered into the age of mobile internet and multi-screen usage (e.g. smartphone, tablets, personal computer, and more). Alongside the widespread adoption of mobile applications during the mobile economy boom, there was a surge in data growth in China's consumer market. In this 'mobile first' and 'mobile only' environment, people began to use their mobile phones heavily to shop for consumer goods, order meal deliveries, buy tickets and pay for almost all daily activities, leaving vast amounts of data on digital platforms.

Now, in the age of artificial intelligence (AI), internet users and tech companies clash with regards to personal data issues more directly than ever. Because data has become a critical resource in AI and data-driven technologies, internet giants are more often *proactively* collecting user data. Furthermore, they are collecting every aspect of user data—whether in the context of identity data, network data, or behavioral data—as illustrated in Figure 1. Take precision marketing, for example. Users' data are analyzed and based on the different characteristic labels they are given (e.g. "makeup lover," "sports fan," or, say, "keen to travel."). Then, companies show specific advertising messages to potential customers based on the matching of labels.

As the "mosaic theory" suggests, disparate items of information—though individually of limited or no utility to the owner—can take on added significance when combined with other items of information. In cyberspace, there is a lot of different information that an individual user would never think could be used to identify him or her as a specific person with specific monetizable preferences. But when a computer algorithm combines the different pieces together, the computer can see connections in ways that humans cannot. When a digital platform combines different sets of data—either from different service lines of the same platform

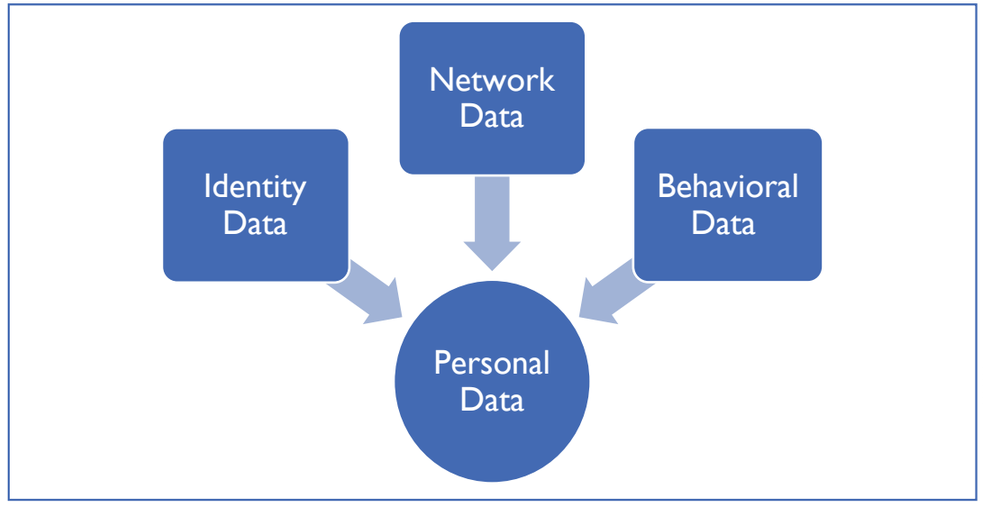

Illustration: ???????

Figure 1: User data: identity, network, and behavioral

or from third-party data vendors in different sectors—the power of user data integration grows exponentially.

Not surprisingly, many Chinese internet giants have expanded their businesses into "super apps." They are active in various areas—from food ordering and taxi hailing to e-commerce and money lending—and they collect and possess massive user data from their numerous activities. For example, Tencent openly vowed to become the fundamental platform for China's internet, the twenty-first-century version of a provider of "water and electricity supplies in daily life." Another major platform, Meituan, covers food ordering, bicycle-sharing, and numerous other everyday services. Consequently, these large platforms can profile their uses in striking detail.

At the same time, these platforms have used big data analysis to provide users with more personalized and faster services. On the other hand, the data power of many platforms has also aroused public concerns that big data could be abused. They quickly learned the importance of data and privacy through "big data killing"—the more personal data the platforms have, the more users have to pay. It is to an explanation of this term to which we next turn.

BIG DATA KILLING

In Mandarin, the word "*shashu*" literally means "killing someone with whom a person is acquainted," and it is a term that has emerged

from China's market economy. It refers to a situation whereby a person takes advantage of another who innocently believes the former is a friend who acts in the latter's best interest.

In the data economy, the concept has evolved into "big data killing" (or *dashuju shashu*) as internet platforms capitalize on information received from regular users whose spending habits become well-known by the platforms. The "killing" refers to the situation in which, for the same goods and services, the price shown to old customers is more expensive than it is for new users. In economic terms, big data killing is a form of price discrimination.

Big data killing illustrates the power and value of data. Because a given internet platform has no knowledge about a new user, it offers a relatively low product (or service) price so that the new user can enjoy the "sweetness" of the first experience (at the same time, the platform gathers his or her personal data through the user's platform registration and related transactions). Meanwhile the same internet platform offers a relatively higher price to existing users for the same product (or service), especially to those who are analyzed as having higher spending power and lower sensitivity to pricing.

Consider online travel agency sites—one sector where big data killing is prevalent. Savvy users have discovered that when they try to book air tickets or hotel rooms, the price is higher for a frequent user of a given website than for a newcomer. Online car-hailing platforms are also found to offer different prices in the same region to different users. A similar phenomenon is also reported to occur in online shopping, online ticket purchases, video websites, and many other fields.

In April 2018, iiMedia Research, a leading data mining and analysis agency based in Guangzhou, released its "2018 China Big Data Killing and User Behavior Report." According to its analysis, 77.8 percent of surveyed internet users indicated that service applications using big data for differential pricing were unacceptable, and 73.9 percent of respondents did not know that internet applications were using big data to categorize different user behaviors. The report suggests that a high percentage of internet users are unaware of such increasingly common industry practice. Many of them are insensitive to prices and are likely to become the target of big data killing.

China's regulators took action as the issue gained social traction. Big data killing is now prohibited by China's E-Commerce Law, which became effective in January 2019. The law provides that when e-commerce operators provide a search result for a good or service, it should simultaneously provide the consumer with an option to see results that do not target his or her identifiable traits.

In other words, merchants could still offer customized services and products to users, but users also have to be provided with the option of seeing general offerings that are not based on personal data preferences. Later in 2019, new administrative rules came into force, which further required that customized recommendations created by algorithms driven by personal information, including news feeds and advertising, needed to be explicitly labeled.

As illustrated by the big data killing example, the notion that Chinese internet users care little about giving up personal data is not true. The more direct reason is that there is still a general lack of understanding as to how data is collected, categorized, and used by internet-based social platforms. Nevertheless, after years of Chinese internet companies building business models around the lack of awareness about privacy by Chinese users, these same users are becoming more knowledgeable, and they are becoming angry with companies abusing their personal information.

Data Privacy Regulations Rising in China

The year 2018 could be hailed as the one when the Chinese public started awakening to privacy concerns. When Facebook CEO Mark Zuckerberg testified before the U.S. Congress in early 2018 with regards to Facebook's data practices, he had warned that regulating the platform's use of personal data would cause the United States to fall behind China when it came to data-intensive innovation, such as AI. As if echoing Zuckerberg's testimony, the founder of China's leading search engine Baidu, Robin Li, commented in a 2018 interview that if Chinese people "are able to exchange privacy for safety, convenience, or efficiency—and in many cases they are willing to do that—then we can make more use of that data."

Ironically, Li's remark was not accepted by the Chinese public. Baidu was sued that year by a consumer rights protection group in Jiangsu province for collecting user data without consent. The lawsuit was later withdrawn after Baidu removed the function to monitor users' contacts and activities.

In the same year of Baidu's litigation, Chinese users challenged other internet giants on personal data privacy issues, including most notably Alibaba. Ant Group, Alibaba's financial arm,

had launched Zhima Credit, an online credit scoring service which offers loans based on users' digital activities, transaction records, and social media presence. Users discovered that they had been enrolled in this credit scoring system by default and without consent. Under pressure, Alibaba apologized.

No doubt, Chinese consumers are increasingly standing up to internet giants with respect to their digital privacy in unprecedented ways, and China is in the early stages of setting up a data protection regulatory system. For instance, the Cyber Security Law, which became effective in June 2017, for the first time included a set of data protection provisions in the form of national-level legislation. Moreover, the 2018 e-Commerce Law incorporated data privacy protections for consumers such as the 'right to be forgotten,' similar to the EU's landmark privacy legislative act, the General Data Protection Regulation (GDPR), which came into effect the same year (more on this point below).

In May 2019, as the Law on Personal Data Protection was being drafted, the Cyberspace Administration of China (CAC)—the country's highest administrative regulator of the internet—issued a document entitled "Measures on the Administration of Data Security." The Measures lay out specific rules regarding the do's and don'ts for how internet companies collect and use customer data. The CAC Measures focused in particular on how users can gain greater control of their data in mobile apps. In parallel, the CAC together with the Ministry of Public Security, the Ministry of Industry and Information Technology, and the State Administration for Market Regulation, launched a national campaign to inspect smartphone apps to determine if they illegally or excessively collect users' information. By July 2019, a group of widely-used apps had been ordered to correct their data collection practices. At the same time, ten apps, including one issued by the Bank of China, were found to have no user privacy rules.

Additionally, in May 2020 China adopted a new Civil Code that took effect in January 2021. Its passage marked a key step forward in developing a legal framework governing individual data privacy. This sweeping package, which included numerous other civil laws, statutorily defined for the first time privacy as a "personality right." The Code devotes an entire chapter to addressing various personality rights—covering individuals' rights to control the commercial use of their name, title, portrait, reputation, and privacy, while adding new articles on protecting personal information.

Still, the ongoing pandemic creates novel data and privacy controversies. Data is being created at a faster-ever rate since the coronavirus virus made everyone's life largely virtual. For example, governments collect a vast amount of individual information to keep close tabs on population health and location data. Under ordinary circumstances, sensitive patient-linked medical records should be kept private, but during this extraordinary crisis governments needed to constantly collect such data, often through private internet platforms, raising concerns about data breach, loss, or unauthorized use.

To that end, China's forthcoming Personal Information Protection Law and its Data Security Law are expected to address these complex issues in more detail. The drafters face tough challenges in balancing the considerations of individuals' personal privacy, enterprises' business development, and national and public security. Since these two laws are working their way through a process of formulation in the National People's Congress, they may soon become effective—a major step towards regularizing this patchwork affair of personal information protection into an integrated, comprehensive framework, as summarized in Table 1.

Year	Name of Law
2017	Cybersecurity Law
2018	E-Commerce Law
2019	CAC Measures on the Administration of Data Security
2020	Civil Code
forthcoming	Personal Information Protection Law; Data Security Law

Table 1: Timeline of China's Data Privacy and Security Legal Framework

ANTITRUST ACTIONS ON BIG TECHS

In addition to data privacy protection (how private data is *collected*), another aspect of data regulation is to control the power of major platforms by antitrust regulations (how collective data is *used*), since their power mostly derives from the accrual of vast databases of user data. Thanks to advanced data analytics, Chinese tech companies are turning into business ecosystems in which sectors that once seemed disconnected are now integrated seamlessly by user data. They are increasingly assuming powerful positions in banking, finance, advertising, retail, and other markets that force smaller businesses to rely on their platforms to reach customers.

It is no coincidence that the antitrust crusades in China have accelerated during the pandemic. A locked-down world has come to rely on tech companies more than ever, with many racking up gains at the expense of smaller

competitors. For example, Meituan's platform dominates online-to-offline (O2O) life service such as food delivery and mobility services. When everyone was ordering take-out during the coronavirus outbreak, Meituan and Eleme cultivated a clan of "virtual restaurants," operating out of ghost kitchens set up for the preparation of delivery-only meals, by providing targeted consumer marketing, as the O2O platforms probably manage the most sophisticated location-based technologies in the market.

It is no coincidence that the antitrust crusades in China have accelerated during the pandemic. A locked-down world has come to rely on tech companies more than ever, with many racking up gains at the expense of smaller competitors.

Of course, the heavyweights charge a significant commission rate for the service. Meituan has gained market share and turned a profit, becoming the third Chinese internet firm—after Alibaba and Tencent—to exceed a $100 billion valuation in the public market in 2020. On the other hand, smaller brick-and-mortar restaurants that rely on e-commerce platforms have found it hard to do the same. Under pressure, Meituan was forced to apologize after a restaurant association accused it of abusing its dominance during the outbreak by requiring merchants to sign exclusive agreements and charging restaurants commissions as high as 26 percent.

In November 2020, the State Administration of Market Regulation (SAMR) issued a Draft Anti-Monopoly Guidelines for Platform Economy. This new document targets anti-competitive behaviors in the internet sector, such as big data price discrimination and exclusive cooperation agreements. This draft followed the aforementioned abrupt suspension of a $37 billion stock offering by Ant Group, the fintech arm of China's internet giant Alibaba, partly due to new regulations relating to the use of consumer data for the offering and issuance of small personal loans. In February 2021, SAMR announced an updated draft guideline document to formalize the earlier draft and clarified a series of monopolistic practices on which regulators plan to crack down.

This represents the first time that China is attempting to define what constitutes anti-competitive behavior in the tech sector: the new anti-monopoly guidelines try to address shortcomings in applying existing antitrust theories to companies like Ant Group. For instance, the guidelines restrict behavior such as price discrimination (the aforementioned big data killing), preferential treatment for merchants who sign exclusive agreements with platforms, and compulsory collection of user data.

Also, the same week in which these new anti-monopoly guidelines were released witnessed another new development, namely the acceptance by the Beijing Intellectual Property Court of a case filing by leading short video platform ByteDance, the parent of TikTok and Douyin apps, against Tencent over alleged monopolistic behavior as defined by those same guidelines. It seems likely that Chinese regulators expect this landmark case to fill in the details of the guidelines, so to speak, given that these still appear to be more of a framework than anything else. According to Bytedance, Tencent had blocked Douyin from its flagship networking apps WeChat and QQ for three years, banning users from viewing or sharing Bytedance content. All stakeholders are paying close attention to this landmark case to get a sense of where all this is headed, as it is poised to become a harbinger of the coming decade of anti-monopoly regulatory and legislative action in China.

Chinese Big Tech firms will likely have to fundamentally rethink the way they do business in the coming decade.

Of course, the SAMR guidelines are, at present, merely administrative regulations. Further to the SAMR guidelines and regulatory actions, China's Anti-Monopoly Law is scheduled to be amended later this year to incorporate more digital economy considerations. Large internet platforms have tended to resist handing over their data—a crucial asset that helps them run operations more efficiently and lure new customers at low cost. They do not share customer data with business rivals, giving them what some call an unfair, monopolistic advantage in their core markets. As such, the amendments to China's Anti-Monopoly Law are expected to address the risk of network and data monopolies. In short, Chinese Big Tech firms will likely have to fundamentally rethink the way they do business in the coming decade. The potentially strategic importance of these expected developments should not be underestimated.

AMERICA MUST CATCH UP

The bottom line is that China is accelerating its digital economy regulations. As the largest mobile internet user market, China's evolving data privacy and security framework will necessarily have profound global implications. China has already built a significant capacity in data centers and AI processing capacity, and it has also become the world's second largest market in cloud computing. At present, China stores about one-fifth of the world's data and—given its commitment to invest heavily in the

"new infrastructure" (the infrastructure of the digital economy)—its share in global data is likely to continue to increase. Because foreign internet giants operate online in China and Chinese companies operate globally, China's cyberspace laws and policies have worldwide relevance.

Thus, China's regulatory actions must be viewed in the context of a global push for more Big Tech regulations. Although geopolitical tensions are ever-present in the emerging post-pandemic world, all the major powers seem to share a consensus on at least one important issue, namely that Big Tech firms (irrespective of where they may be headquartered) are too big, too powerful, and too profitable. And that global focus is only likely to intensify, driving governments everywhere to take such companies to court, implement strict local data rules, and pass new competition laws.

Because foreign internet giants operate online in China and Chinese companies operate globally, China's cyberspace laws and policies have worldwide relevance.

Certainly, the EU is another leading force. Its aforementioned General Data Protection Regulation has fundamentally changed the way data is handled globally after it came into force in 2018. The GDPR has forced global companies to reconsider their data policies, inspiring countries far and wide—from Brazil to India—to develop their own data privacy regulations based on a de facto GDPR benchmark. At the antitrust front, the EU has chased Facebook, Google, and Microsoft for years. It should be noted, however, that at least so far what the EU has accomplished is likely not enough. Even the high fines the EU has imposed on U.S.-headquartered Big Techs firms have not significantly changed market dynamics.

By contrast, the United States—which was once a global leader in internet regulatory policy—has come to lag far behind China (and the EU) in recent years. Today, America is no longer at the forefront of drafting privacy regulations. China's new data privacy laws may stimulate the United States, which still has no national-level position on data protection, to expedite relevant legal measures. On antitrust, China's actions against Ant Group shows that Beijing has been much more effective in curbing the dominance of Big Tech companies than the United States (or even the European Union), which has done little to rein in Amazon, Apple, Facebook, and Google.

America's tech concentration crisis did not emerge in the Trump years, although it certainly deepened during his four-year term in office. The Trump Administration failed to make Big Tech regulation a strategic priority. As such, notwithstanding how American tech companies may subjectively feel, they have in truth been enjoying a very high phase of innovation thanks to little U.S. federal government regulatory oversight. It seems clear that the United States needs a new rulebook for the tech sector. As a result, the Biden Administration must choose between taking a new, "digital era" view of antitrust law to rein in or break up Big Tech firms; sticking with a laissez-faire approach that critics say has led to the "curse of bigness"; or trying to find some middle path.

In this new antitrust era, Chinese examples may provide important reference points to the emerging generation of U.S. antitrust experts that look beyond the hoary concept that higher prices are the primary gauge of competitive harm.

This is a major project. Fortunately, widespread concern over the power of Big Tech is in the air, and on the hardest tech policy issues (privacy, competition, and content) a bipartisan consensus seems to be building up amongst U.S. lawmakers. In a reversal from a general embrace of tech giants, the Biden Administration appears to be willing to put three critical elements—federal privacy law, standards for the collection and use of personal information, and a robust new competition policy regime—together as a coherent national policy. Furthermore, the Biden Administration may also find itself expressing an interest in beefing up America's antitrust and data-enforcement agencies, as enforcing technically complex rules is even harder than passing new laws for the new economy.

In this new antitrust era, Chinese examples may provide important reference points to the emerging generation of U.S. antitrust experts that look beyond the hoary concept that higher prices are the primary gauge of competitive harm. For decades, antitrust reviews have employed a "consumer welfare standard" that focused on pricing power. This no longer applies to the digital economy because the biggest tech companies have established trillion-dollar monopolies by charging consumers next to nothing. In fact, many platforms in China often doll out cash rebates to netizens in order to incentivize them to use the mobile applications.

But individuals are not just consumers—they are also workers, entrepreneurs, and community members. In practice, as industries consolidate, consumers sometimes pay less for products, but wages also stagnate and

entrepreneurship is stifled. Therefore, China's new antitrust thinking suggests that the more important consideration should be given to data privacy, data usage, and the overall impact on smaller companies. (Yes, compared to Tencent, Bytedance is a smaller company, even though it is the highest valued private media company with more than $100 billion valuation.)

Due to the fact that to a large extent the cyberspace-based digital economy remains undefined, the data law framework has become intertwined into broader geopolitical considerations. Whichever country (or block) will be able take the lead in achieving breakthroughs in legislation will to a large extent be able to provide a model for the next-generation of internet usage. Subsequently, this country (or block) is likely to have more leadership power whenever a digital economy version of WTO rules is eventually formed by nations. That is why more and more people are talking about what the China model could represent.

Whichever country (or block) will be able take the lead in achieving breakthroughs in legislation will to a large extent be able to provide a model for the next-generation of internet usage.

In the EU world, GDPR is so far not explicitly tied to more far-reaching goals regarding national security and social stability. However, in February 2020 Brussels unveiled a plan to restore what its officials called "technological sovereignty," which aims to boost the EU's digital economy and avoid the block's overreliance on non-EU companies. As such, new laws to reflect more "data sovereignty" considerations can be expected to emerge in the EU space. Furthermore, China's framework may also provide a reference point for major emerging economies such as India, Brazil, and the ASEAN countries when they look to regulate cyberspace activities and emerging technologies. The United States may still hold a leadership in the digital economy, but it will need to quickly take major regulatory actions on Big Tech firms to stay in the game.

Global Collaboration

Big Tech regulation is new territory for legislatures all over the world—not just in China, the EU, and the United States. There is thus a great deal of uncertainty as to the eventual form of governmental policy and its impact on global business operations. While there is a general consensus that heightened regulation is needed, a major risk lies in the failure of the Chinese regulatory framework (or the EU's recently proposed Digital Markets Act and Digital Services Act) to become an effective global standard and instead serving to legitimize bad regulatory practices in other countries. Governments must enhance cooperation across national competition agencies to address competition issues that are increasingly transnational in scope.

It would be extremely positive for the global digital economy if the major digital economies—namely, the United States, China, and the EU—could collectively develop a regulatory framework on Big Tech companies. At the January 2021 Annual Meeting of the World Economic Forum in Davos, Chinese President Xi Jinping called for the world to work together to tackle global challenges. For that, collaboration on Big Tech regulation is critical to sustain the momentum of global tech innovation. The coming decade will almost certainly redefine the digital economy. Hopefully for the better.