ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

May 11, 2017

Beijing Dongcheng District
Chaoyang Gate Street
State Internet Information Office
Cybersecurity Coordination Bureau
Beijing, China, 100010

Dear Sir or Madam:

On behalf of the Information and Technology and Innovation Foundation (ITIF), we are pleased to submit these comments in response to the State Internet Information Office's request for public comments on the draft "Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security," which was released on April 11, 2017. ITIF is grateful for the opportunity to provide feedback.

ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation, and pro-technology public policy agenda that spurs growth, prosperity, and progress. ITIF frequently engages with technology companies and policymakers from China and around the world and has done extensive research and analysis of public policy and technological innovation issues in China. ITIF is based in Washington, DC.

Yours sincerely,

Dr. Robert D. Atkinson
President and Founder, Information Technology and Innovation Foundation
ratkinson@itif.org

Nigel Cory
Trade Policy Analyst, Information Technology and Innovation Foundation
ncory@itif.org

OVERVIEW

China's policy on data and technology issues has been changing rapidly in recent years as it aims to develop data-intensive and high-technology sectors of the economy, as outlined in China's 13th Five-Year Plan (2016-2020) and other plans, such as the "Internet Plus" policy. At the heart of China's plans is the recognition that data will play an increasingly critical role in driving innovation and economic competitiveness. The draft "Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security" (herein referred to as "the circular") will greatly expand the scope of local data residency requirements—also known as data localization—as well as measures that inhibit the seamless collection, use, and transfer of data. By increasing the cost and complexity of data management and cross-border transfers of data, the circular will undermine China's ability to benefit from data-driven innovation.[1]

This draft circular, if implemented in its current form, will not only undermine Chinese firms' own ability to use data to innovate, but also will discriminate against foreign technology firms who will be forced to set up or use duplicative computing facilities and be constrained in how they use data. Foreign technology companies have considerable experience and technology that could help China develop a dynamic and competitive data-intensive and innovative economy. However, this draft circular and a range of other recent laws and regulations discriminate and disadvantage foreign firms, thereby limiting their ability (and their willingness) to operate in China. China's rapidly changing regulatory environment has further raised a number of serious concerns about the role that foreign technology firms will be allowed to play in China in the years ahead.

OUTCOME, NOT PROCESS: THE CIRCULAR'S MISGUIDED FOCUS ON LOCATION

Securing the digital environment requires constant vigilance. Using the Internet and data to achieve economic and social objectives will always require accepting a certain level of digital security risk, which can be mitigated through targeted privacy and security measures. But since there is a cost associated with these measures, countries need to aim for balance—overly restrictive policies will limit their ability to (continue to)

[1] Analysis based on an unofficial translation of the circular: "Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security (Draft for Soliciting Opinions)," *China Copyright and Media,* April 26, 2017, https://chinacopyrightandmedia.wordpress.com/2017/04/11/circular-of-the-state-internet-information-office-on-the-public-consultation-on-the-measures-for-the-assessment-of-personal-information-and-important-data-exit-security-draft-for-soliciting-opinions.

derive enormous economic and social benefits from technological innovations, including the use of data. China's intentions to address emerging issues around data, such as privacy and cybersecurity, are understandable and shared by many countries around the world. However, the circular creates an unbalanced framework for managing data as it focuses on process and the location of data and not on outcomes (whether this is privacy- or cybersecurity-related). Measures designed to address privacy or cybersecurity issues need to be appropriate and commensurate with the technology and the economic and social issues at hand—addressing the relevant issue without undermining the use of the technology.[2]

Yet the circular's main result will be to greatly expand the scope of costly and restrictive data localization requirements. These localization requirements will have a negative impact on China's entire economy as it will apply to so many types of data and to so many companies that manage such data. First, these requirements are likely to apply to most companies in China as the circular will likely cover a large amount of the data generated in China—given it applies to companies that manage personal data about Chinese citizens and those that manage any "important data" from China, which the circular defines as data related to national security, economic development, and social and public interests. Second, the circular ensures it will apply to a broad range of the economy as it applies to "operators" of "critical information infrastructure." Network operators could be any company collecting information in China given the definition that it covers "owners, managers, and network service providers of network."

Furthermore, the circular reinforces this preference for keeping data in China by making it difficult for companies to transfer data overseas. First, the circular only allows the transfer of relevant data overseas if there is a business need to do so. Modern businesses transfer data as a matter of course, so any measure that tries to define or limit this undermines the business itself and makes businesses—foreign and domestic—less efficient and competitive. Second, the circular subjects any potential data transfers to a "self-security assessment." The circular requires companies to report on specific and technical details about the amount, scope, type, and sensitivity of the data and details about the specific recipient and the potential for such transfers to affect the vague and broad-ranging set of "national security, social, and public interests." This assessment, especially the final catch-all category, creates significant uncertainty for companies that may want to transfer data overseas as these rules provide Chinese regulators with the unconstrained ability to claim that a company did not comply

[2] Organization for Economic Cooperation and Development (OECD), "Managing Digital Security and Privacy Risk," (Paris: OECD, 2016), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En.

and to stop any data transfers. Furthermore, the circular's self-assessment places costly and unreasonable burdens on companies trying to transfer data overseas. It requires companies to explain to the data subject (who the data with personal information pertains to) the purpose, scope, content, recipient, and destination country and to get their consent.

On top of this, the circular erects further barriers for a potentially large range of businesses by requiring them to report to regulators in order to organize a security assessment if the data they want to transfer falls into a vague and expansive list of categories. For example, if the data being transferred is over 1,000 GB, if the data involves population health, large-scale engineering activities, the marine environment, and sensitive geographic information, and if the data could affect national security and social and public interests. Given the volume and frequency of data transfers for modern businesses, especially those with global operations, such vague and arbitrary inspection and assessment requirements inject uncertainty, delays, and costs into a core business activity.

THE MISTAKEN LINK BETWEEN LOCAL DATA STORAGE AND PRIVACY/CYBERSECURITY

Most concerningly, the draft circular perpetuates the mistaken belief that many policymakers hold that data is more private and secure when it is stored within a country's borders. However, in most instances, data-localization mandates do not increase commercial privacy or data security.[3]

What the circular does not recognize is that companies cannot escape a country's privacy or cybersecurity requirements by transferring data overseas. Most companies doing business in a nation—all domestic companies and most foreign—have "legal nexus," which puts the company in that country's jurisdiction. For example, a German bank or manufacturer that has branches or plants in China is subject to China's privacy and security laws and regulations. As such, the bank must comply with those rules whether it stores the data in China, in Germany or even in a third country. Companies simply cannot escape from complying with a nation's laws by transferring data overseas.

The circular mistakenly focuses on geography to solve privacy and cybersecurity concerns. China's government should instead focus on ensuring that individuals and companies have the legal tools they need to protect their data and that the government has the ability to monitor and enforce these tools. In many countries around the world, consumers and companies can rely on contracts or laws to limit voluntary

[3] Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

disclosures to ensure that data stored abroad receives the same level of protection as data stored at home. In the case of inadvertent disclosures of data (e.g., security breaches), to the extent nations have security laws and regulations, again a company operating in the nation is subject to those laws, regardless of where the data are stored. Moreover, security breaches can happen no matter where data are stored—data centers everywhere are exposed to similar risks. Such disclosures are the result of security failures, such as hackers breaking into a corporate network to steal data, government agencies tapping into telecommunications links, or employees mistakenly posting sensitive data in a public forum. What is important is that the company involved (either a company with its own networks or a third-party cloud provider) be dedicated to implementing the most advanced methods to prevent such attacks. The location of these systems has no effect on security. If anything allowing companies to store data with global best-in-class cloud service providers, even if not in China, improves security as these cloud providers have the strongest motivation in having secure systems and the strongest technical and managerial capabilities to operate secure systems.

Moreover, this circular reflects a common misunderstanding pertinent to data security. The confidentiality of data generally depends not on which country the information is stored in, but on the measures used to store it securely. A secure server in Colombia is no different from a secure server in Brazil. Data security depends on the technical, physical, and administrative controls implemented by the service provider, which can be strong or weak, regardless of where the data is stored. For example, in a practice that protects both data privacy and security, some cloud-computing companies have upgraded security controls so that customers retain the keys used to encrypt data before it is uploaded, thereby preventing third parties, including the cloud companies themselves, from accessing their data.[4] While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any service provider, cloud computing will likely lead to better overall security because implementing a robust security program requires resources and expertise, which is what many small- and mid-sized organizations lack, but large-scale cloud-computing providers can offer.

PUTTING DATA INNOVATION AT RISK

From an innovation perspective, the circular is fundamentally flawed by taking a precautionary approach that first asks why data should flow, instead of targeting specific problems, while ensuring that data is still able to flow across borders freely. The circular holds potentially significant social and economic risks given the growing importance of data innovation—the increased use of large and disparate volumes of data and

[4] Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law" (Information Technology and Innovation Foundation, March 2016), http://www2.itif.org/2016-unlocking-encryption.pdf.

analytics to significantly improve or foster the development of new products, processes, organizational methods, and markets. Such data-driven innovation can create significant added value to a variety of operations, ranging from optimizing and reengineering the value chain and manufacturing production to more efficient use of resources, better customer relationships, and the development of new markets.[5] In this new economic model, which Chinese leaders aspire toward, data are a core asset that can create a significant competitive advantage and drive innovation, sustainable growth, and development.

The draft circular would severely affect how companies can collect, analyze, and use data, including personal data, in new and innovative ways to address social and economic issues. For example, this puts at risk China's ability to use data-driven innovation to address local and global challenges, such as climate change, chronic disease, food production, and energy security. Such technologies rely on an open and interconnected digital environment that allows organizations and individuals to move data easily, flexibly, and cheaply among different partners, systems, and borders. The draft circular would inhibit this process by creating a closed and stifled digital environment as opposed to an open and dynamic one.

The circular would be particularly detrimental to how firms in China use personal data, which is a central part of the modern digital economy. Consumers' personal data is collected and analyzed in a number of ways. Consumer data is provided or revealed by choice, such as through email and social media; through compulsory disclosure, such as to receive a service; without explicit consent, for example, by tracking an individual's web browsing habits; and through the sensors in everyday technology, such as smartphones, laptops, wearable technology, and Internet-connected household items, such as cars, homes, and offices. Companies collect and analyze large amounts of consumer data to predict tends, such as changes in consumer demand and individual preferences, which they can use to inform future business decisions about advertising, pricing, inventory, research and development, and product redesign. Furthermore, the circular's requirement that companies wanting to transfer data must explain the purpose of the transfer restricts organizations from conducting unrelated post hoc analysis to develop new types of products and services based on what they learn from the data, even if these organizations use this data in a way that protects individual privacy.

The circular would also reduce companies' ability to access data on a nearly real-time basis. The speed at which data are generated, accessed, processed, and analyzed is critical to many modern business services. Companies and policymakers now rely on constant access to data to make real-time "nowcasts" ranging from

[5] OECD, "Managing Digital Security and Privacy Risk."

purchases of cars and consumer goods to flu epidemics to employment/unemployment trends in order to improve the quality of policy and business decisions.[6]

Furthermore, the circular would make data management significantly harder and more inefficient, especially that which is involved in "big data." A characteristic of leading firms is their ability to analyze a number of diverse and unstructured data sets, such as those sourced from web browsing logs, social media, mobile communications, sensors, and financial transactions. Companies need to be able to seamlessly link large and diverse data sets, which may be highly context dependent, thereby making individual datasets useless without a broader set of data points. As opposed to previously labor-intensive processing, big data analytics allows companies to extract valuable insights from the huge amounts of unstructured data they may have. The circular's impact on this process may have significant implications for a company's ability to use data to innovate—estimates suggest that the share of unstructured data in businesses could be as high as 80 to 85 percent and remain largely unexploited or underexploited.[7] But to do this, companies need to be able to seamlessly transfer, link, and process data in an automated, timely, and cost-effective manner.

PUTTING AT RISK THE GLOBAL AMBITIONS OF CHINESE MULTINATIONAL FIRMS

China's large and fast growing economy is home to a growing number of firms that also have global ambitions, whether in the digital economy or technology sectors, such as Alibaba, Tencent, Baidu, and Huawei, or in traditional sectors, such as manufacturing and resource extraction. As these firms enter international markets, often with the government's support as part of "going out" campaigns to turn domestic firms into true multinational competitors, they will need to move data around the world in order to be competitive with other multinational companies, who rely on data flows to manage global operations as efficiently as possible and to drive innovations in their products, services, or organizational structure.[8] This draft circular would affect the ability of these firms to manage such global data flows.

---

[6] Hyunyoung Choi and Hal Varian, "Predicting the Present with Google Trends" (discussion paper, Google, April 10, 2016); Yan Carrière-Swallow and Felipe Labbé, "Nowcasting with Google Trends in an Emerging Market" (working paper, Central Bank of Chile Working Papers, No. 588, July 2010).

[7] Organization for Economic Cooperation and Development (OECD), "Exploring Data-Driven Innovation as a New Source of Growth" (Paris: OECD, 2013), http://www.oecd-ilibrary.org/docserver/download/5k47zw3fcp43-en.pdf?expires=1494445605&id=id&accname=guest&checksum=0F38AB0358074F5AC3F7078D126A5729.

[8] Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries: (The Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-cross-border-data-flows.pdf.

Even if China's own data localization measures do not directly affect its own multinational firms (assuming it doesn't interfere in their transferring of non-Chinese data back to China for storage and analysis), it could spur other nations to prohibit Chinese firms from transferring data from their respective countries back to China (perhaps due to similar privacy or cybersecurity concerns). In essence, it could lead to a domino effect. Ultimately, the data localization requirements in this draft circular, along with localization policies in other countries, contribute to the fragmentation, or "Balkanization," of the Internet by misguidedly focusing on location when dealing with data-related issues.

RECOMMENDATION: INTEROPERABILITY—A GLOBAL AND OPEN VS. A LOCAL AND CLOSED FRAMEWORK FOR DATA FLOWS

China is obviously free to pursue privacy based on its own cultural and social values, as is every country. The circular is obviously part of China's emerging data privacy framework. As we've seen in the debate around cross-border data flows and data protection between the United States and the European Union, while both sides have different approaches to privacy, both can still seek and find common objectives and mutually acceptable ways to protect privacy of the individual while minimizing the burdens imposed on businesses and other organizations. China should join in similar international efforts to establish a framework that protects data privacy while allowing data to flow freely. While the circular acknowledges that China may enter into agreements with other countries on data transfers from China, it essentially precludes most data transfers by making data localization a requirement for so many different types of data and by making any transfers so difficult.

China should instead focus on actual measures that improve privacy and engage in international forums related to efforts to develop interoperability with other privacy systems so that a comparable level of privacy is achieved wherever the data is stored. Much as regulators for food production and safety, medical devices, and pharmaceuticals have worked together to facilitate mutual confidence and understanding and more consistent decisions and policies by developing a common understanding about core principles, concepts, and processes involved in managing the risks in these areas, the same can be done for data privacy. As the Organization for Economic Cooperation and Development writes, "Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global

interoperability can help simplify compliance by organizations and ensure that privacy requirements are maintained."[9]

One possible mechanism for China to consider is the Asia Pacific Economic Community's (APEC's) Cross-Border Privacy Rules (CBPR) system, which is "designed to protect the privacy of consumer data moving between APEC economies by requiring companies to develop their own internal business rules on cross-border data privacy procedures."[10] This complementary regulatory policy limits costs to businesses while protecting data privacy, which is critical to facilitating this process.[11]

[9] Organization for Economic Cooperation and Development (OECD), "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (Paris: OECD, 2013), 34, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[10] See "The Cross Border Privacy Rules System: Promoting Consumer Privacy and Economic Growth Across the APEC Region," Asia-Pacific Economic Cooperation, September 5, 2015, http://www.apec.org/Press/Features/2013/0903_cbpr.aspx. The CBPR is a voluntary, certification-based system that promotes a consistent baseline set of data privacy practices for companies doing business in participating APEC economies. Company privacy policies are to be audited by APEC-recognized Accountability Agents. See Asia-Pacific Economic Cooperation, "Promoting Cooperation on Data Transfer Systems Between Europe and the Asia-Pacific" news release, March 6, 2013, http://www.apec.org/Press/News-Releases/2013/0306_data.aspx.

[11] "APEC expands data privacy system to protect consumers," Asia-Pacific Economic Cooperation (APEC) website, last accessed May 11, 2017, https://www.apec.org/Press/News-Releases/2014/0501_CBPR.aspx.