

May 11, 2017

National Internet Information Office, Network Security Coordination Bureau  
Beijing Dongcheng District  
Chaoyang Gate Street 225  
100010  
People's Republic of China

Submitted via email ([security@cac.gov.cn](mailto:security@cac.gov.cn))

RE: Comments of ACT | The App Association regarding the Cybersecurity Administration of China's *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)*

Dear Sir/Madam:

ACT | The App Association (the App Association) appreciates the opportunity to provide input to the People's Republic of China's (PRC's) Cyberspace Administration of China (CAC) on its draft of the "Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data" (the Draft Measures) for inclusion in its recent Cybersecurity Law.<sup>1</sup>

The App Association represents more than 5,000 small business application developers and connected device companies, located both within the People's Republic of China and across the globe. These companies drive an app economy worth more than \$143 billion<sup>2</sup> which continues to grow. App Association members leverage the connectivity of smart devices to create innovative solutions that make our lives better. The App Association is the leading industry resource on market strategy, regulated industries, privacy, and security.

---

<sup>1</sup> Draft Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Important Data (promulgated by the Cyberspace Administration of China, April 11, 2017) (Draft Measures).

<sup>2</sup> <http://actonline.org/2017/04/20/state-of-the-app-economy-report-outlines-growth-dynamism-of-the-app-ecosystem/>.

Mobile app companies, regardless of their size or location, must participate in the international digital economy. They rely on the ability to share data across physical borders, and nearly every app is available in stores and platforms outside of their country of origin. As a result, most of the laws that govern how state agencies can access personal electronic data and communications are out of step with the technology consumers use to transmit them. It is imperative that governments attempting to regulate this space do so thoughtfully and carefully; balancing the consumers' rights with facilitating an environment for small business to innovate.

Government mandates to store, route, process, or otherwise use data within the territory of a country contribute to the fragmentation of the digital economy and the internet. Small app development companies do not have the resources to build or maintain unique infrastructure in every country in which they may do business, and they are effectively excluded from commerce by such requirements. The Organisation for Economic Co-operation and Development (OECD) recently published a detailed study establishing that localization requirements cause serious declines in imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification.<sup>3</sup> In addition, the European Centre for International Political Economy (ECIPE) has determined that a data localization requirement in Indonesia would cause a gross domestic product (GDP) loss of 0.7 percent.<sup>4</sup> In the PRC, data localization requirements would be particularly damaging to small- and medium-sized businesses that need unfettered access to the global digital economy to grow.

The App Association further submits the following specific input on draft Articles in the Draft Measures. Based on our concerns, we urge the CAC to indefinitely stay the implementation of this regulation until a future date before which the significant issues in the Draft Measures are resolved through work with affected stakeholders (including the App Association).

---

<sup>3</sup> Stone, S., J. Messent and D. Flaig (2015), "Emerging Policy Issues: Localisation Barriers to Trade", OECD Trade Policy Papers, No. 180, OECD Publishing, Paris.  
<http://dx.doi.org/10.1787/5js1m6v5qd5jen>.

<sup>4</sup> Bauer, et al (2014), "The Costs of Data Localisation: Friendly Fire on Economic Recovery", ECIPE Occasional Paper, No. 3/2014, available at  
[http://www.ecipe.org/app/uploads/2014/12/OCC32014\\_1.pdf](http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf).

## **Article 2**

Article 2 of the draft provides that the personal information and important data collected and generated by the network operator in the operation of the PRC shall be stored in the territory; and for businesses not located in the PRC that a safety assessment shall be carried out. This provision, as proposed, would create significant barriers for members of the App Association seeking to enter the PRC's market through its de facto imposition of a data localization requirement. Coupled with the uncertainty regarding what such a PRC-administered safety requirement would entail, this requirement effectively excludes the innovation of the app economy from the PRC.

## **Articles 7-9**

Articles 7-9 describe the safety assessment a foreign company would undertake when transferring personal information and important data it has collected. The Draft Measures provide considerable confusion as to how and when a business is in violation of its provisions. Article 7 requires companies to perform a self-evaluation assessing the integrity of its data security framework in relation to overseas transfers. Through unhelpfully vague language, this portion of the Draft Measures causes further confusion when one considers CAC's inarticulate definitions in Article 17 and guidance as codified in Article 8—the provisions establishing what information the companies should protect.

In Article 8's current form, a network operator would be required to monitor every ebb and flow of individual data to determine whether such data leaves China, a technically infeasible and cost-prohibitive responsibility for small business innovators that rely on the efficiencies of distributed cloud computing services.

Further, should a company itself be in breach of Article 8 and, thus, subject to an Article 9 review by a PRC regulator, the Draft Measures are unclear as to which regulator would hold domain, another layer of uncertainty which would further limit the number of firms entering into the market, leaving PRC consumers with fewer choices in the app market.

We respectfully request CAC to clarify the above-described issues with Articles 7-9 before putting finalizing the Draft Measures.

## **Article 10**

Article 10 provides that the safety assessment organization shall complete the assessment of a network operator within 60 working days, and that the safety assessment shall be transmitted back to the network operator in a timely manner and reported to the national network. The App Association urges the CAC to permit a reasonable amount of time for the completion of risk assessments. Therefore, we

request that at least 120 days be permitted for a safety assessment organization to complete the assessment of a network operator.

### **Article 11**

Article 11 provides categories of data that shall not be permitted to leave the PRC. We again note our objection to such a requirement as the advent of secure cloud computing services can provide for needed data security without locating data inside a geographic area or within a national border. However, the categories of data proposed by the CAC are vague and overbroad and would, in practice, have the effect of balkanizing the PRC from the global internet. In particular, the App Association does not believe it to be technically or economically feasible to store and process all personal information of PRC citizens held without the consent of the subject (or which may be averse to the interests of that individual). We therefore urge the CAC to strike provision (A) from Article 11.

### **Article 12**

As drafted, Article 12 would have a business undertake a safety assessment whenever there is any change whatsoever to when the data receiver changes the destination, scope, quantity, type of data, or when a major security incident occurs, etc. Such a requirement would be extremely burdensome and expensive to the small business innovators that the App Association represents. We therefore request that the CAC provide clarity as to when a safety assessment must be undertaken and to have this threshold rest at an objective metric, such as time period. Such a metric would provide certainty in compliance requirements for businesses, and it would relieve these businesses of having to guess whether a change to their operations or an incident is “significant” enough to merit a re-assessment.

## **Article 17**

Due to its unclear definition of a “network operator” under Article 17, the App Association is concerned that the CAC included app developers in its definition. Article 17 states that a “network operator” is the “owner of the network, network managers and service providers.”<sup>5</sup> This is a sweeping definition encompassing many in the app economy. If the CAC moves forward on a “one size fits all” regulatory approach in the Draft Measures, the Draft Measure’s requirements for “network operators” to store their data in the PRC could significantly harm Chinese consumers by creating burdens that small business innovators cannot afford to bear, effectively excluding them from the market. Chinese consumers are directly impacted by this requirement because of its stifling effects on competition, both internationally and locally, due to these small businesses having to invest an untenable amount capital to ensure they are complying with the law.

Additionally, it is unclear what the CAC means when employing the phrase “important data” as defined in Article 17. The Article defines “important data” as “data closely related to national security, economic development, and social and public interests...”<sup>6</sup> The App Association believes this definition to be overbroad, making it difficult for smaller companies to comply with the law. This is especially worrisome for the app community because of the multilateral and transient nature in which these data-sharing enterprises engage. This potentially onerous measure would place an extraordinary burden on small app companies in the PRC and would make it infeasible for said Chinese companies to compete internationally. If the CAC does not intend to include app developers, then it should provide further guidance on what constitutes a “network operator” and their corresponding obligations, if any. In either event, the CAC should provide further guidance on this issue before effecting these laws.

---

<sup>5</sup> Draft Measures Art. XVII

<sup>6</sup> See *id.*

We therefore respectfully urge CAC to carefully consider the App Association's input on its interim regulations and indefinitely stay the implementation of this regulation until after the significant issues in the Draft Measures are resolved through work with affected stakeholders (including the App Association). The App Association is committed to working with regulators around the globe to bring the benefits of the dynamic app economy to all consumers, including those in the PRC. We urge you to contact us using the information below with any concerns or questions.

Sincerely,



Morgan Reed  
President  
mreed@actonline.org

Brian Scarpelli  
Senior Policy Counsel  
bscarpelli@actonline.org

Joel Thayer  
Associate Policy Counsel  
jthayer@actonline.org

ACT | The App Association  
1401 K St NW (Ste 501)  
Washington, DC 20005  
United States