NUS National University of Singapore | EAI EAST ASIAN INSTITUTE NATIONAL UNIVERSITY OF SINGAPORE

EAI COMMENTARY No. 18 16 September 2020

China's New Data Security Initiative

By Bert Hofman

Data security and trade in data have become a major bone of contention between the United States and China in a conflict that started as a trade tussle but is rapidly sliding towards a new cold war.

Concerns over access to data by the Chinese government has led the United States to impose measures on companies that supply US technologies to Huawei, a leading Chinese telecoms company. It has also lobbied countries around the world to exclude Huawei from their 5G network for reasons of data security risks.

In August, the Trump administration announced that for national security concerns, it would ban the highly sought-after video sharing TikTok app, which is all the rage with teens for showing off their latest dance moves. A similar move was announced for WeChat, another popular app that allows users to perform multiple tasks, from communications to ecommerce to payments. It is a backbone app in China's economy but largely used as a communications tool elsewhere.

The argument was that both apps could divert data of US citizens to the Chinese government. The purge of the two apps was part of the United States' "Clean Network" initiative, which, according to statements by the US State Department, has already signed up more than 30 countries, a claim that remains unverified.

DATA PROTECTION IS GAINING GROUND, ALSO IN CHINA

China itself tightly controls and censors its cyberspace through the Great Firewall and has banned access of major US firms such as Twitter, Facebook and Google.

Its 2017 cybersecurity law raised concerns about the protection of personal data as the law requires companies in China to hand over data if requested by the authorities. The establishment of the Social Credit Schemes aimed at providing individuals with incentives for good behaviour, and which relies on large data collection efforts, has further raised the concern on personal data protection in China. The EU Chamber of Commerce also raised issues with China's overall cybersecurity legal framework, claiming it to be a barrier to entry.

It therefore came as a bit of a surprise that on 8 September Foreign Minister Wang Yi announced an initiative to establish global standards on data security. Wang Yi said that China wanted to promote multilateralism in the area at a time when individual countries were "bullying others and hunting companies". "Global data security rules that reflect the wishes of all countries and respect the interests of all parties should be reached on the basis of universal participation by all parties", Wang said.

China's initiative calls for participating countries to refrain from large-scale surveillance of other countries or illegally acquiring information of foreign citizens through information technology. It also calls for technology firms to stop creating so-called backdoors in their products and services that could allow data to be obtained illegally, as well as for participants to respect the sovereignty, jurisdiction and data management rights of other countries.

Wang Yi also said that China's government "has not and will not require Chinese companies to provide overseas data to the Chinese government in violation of the laws of other countries", thereby countering one of the biggest arguments the United States and others have used to taint data handling by Chinese companies.

WHY THE NEED FOR INTERNATIONAL STANDARDS?

As a frontrunner of the digital economy, most notably ecommerce and digital finance, China needs personal data and information protection. Data protection is important for the development of the digital economy, but getting it right is key: too little of it could undermine markets due to the distrust of providers, while excessive protection can unduly burden businesses and reduce the supply of services (UNCTAD, 2016).

Governments the world over are concerned that data, if mishandled and in the wrong hands, could endanger national security. Even trickier is the movement of data across borders. This is essential for modern trade in services and innovation in manufacturing, which relies on information from users. Keeping data strictly national or localised would impede trade and innovation.

Many countries have taken legal or regulatory steps to protect personal data. On last count, about 140 countries have some form of law or regulation on data protection (Greenleaf and Cottier, 2020). The EU's General Data Protection Regulation is one of the better known and strictest frameworks, which is increasingly becoming a model for other countries to follow.

China enacted its cybersecurity law in 2018, which was skewed towards national security rather than personal data protection. Since then, though, the country has also made efforts to safeguard personal information security and data security; a draft Data Security Law was released for comments in July 2020. The first civil code in China, released in 2020, also specifies data privacy as a personal right.

The data security standards embedded in these laws vary considerably from country to country as different societies have different attitudes on data protection vis-à-vis other societal goals such as development or community interest.

The debate on tracing apps to contain the COVID-19 pandemic illustrates this diverse attitude: countries such as Singapore, Korea and China have quickly adopted or mandated tracing apps to easily locate people who may have had contact with COVID-19 cases. In many European countries and in the United States, such apps were seen to infringe on personal freedom and personal information, and they were of less widespread use.

The digital economy is transnational in nature and allowing data transfers from one country to another can maximise the potential and minimise costs (ITU and World Bank 2020).

Transferring data from one country to another could undermine protection granted to data subjects under national law, leading data protection regimes to impose rules on data transfer to other countries. Such rules obviously have trade implications.

These regulations could be used to protect one's own industry, and could become a barrier against international trade and investment. The WTO's General Agreement in Trade in Services (GATS) has in place some rules on data protection and data transfer, but these were largely formulated before the digital revolution took off in earnest.

A new multilateral agreement on data security and transfer would therefore be highly desirable, but in today's atmosphere the idea seems further off than ever.

Bilateral trade agreements have started to fill the gap and the recent Singapore-Australia Digital Economy Agreement is a case in point. It aims to set "new global benchmarks for trade rules, and a range of practical cooperation initiatives, to reduce barriers to digital trade".

At the same time, a bilateral approach to the complex issues of data protection and data transferability risks a multitude of norms and standards across jurisdictions, which could create high compliance costs for business, especially small and medium-sized enterprises.

CHINA'S INITIATIVE FACES AN UPHILL BATTLE

It is in this context that China proposes global standards on data security. Such standards, once agreed on by a plurality of countries could guide individual countries to develop their own legal framework and become a benchmark for bilateral or multilateral agreements on the topic.

Wang Yi had foreshadowed the initiative at an online G20 meeting the week before the announcement to gain support from this group of influential countries.

China's multilateral approach is going head to head with the United States' Clean Network Initiative. The US initiative seems largely targeted at China: "The Clean Network program is the Trump Administration's comprehensive approach to guarding our citizens' privacy and our companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party (CCP)", a US State Department announcement on the initiative reads.

In August, the Internet Society, an industry group with members including Google, COMCAST, AT&T and Eriksson, sharply criticised the Clean Network Initiative.

"Policies like these only increase the global momentum towards a "Splinternet" — a fractured network, rather than the Internet we have built over the last four decades and need now more than ever", the society wrote in a statement on their website.

Irrespective, little support for China’s initiative can be expected from the United States at this point in time. Other countries have yet to express their views, but it seems unlikely that all G20 members would agree to discuss China’s initiative at this stage.

Nevertheless, China’s initiative could entice other countries to develop their own proposals and principles that may be supported by a broad set of countries. The superpowers could then decide whether they want to get on board with those principles in due course.

Bert Hofman is Director of the East Asian Institute at the National University of Singapore.

EAI commentaries serve to provide quick insights on current topics, based on ongoing research. The opinions expressed in the commentaries are those of the authors and do not necessarily reflect those of the East Asian Institute, or its Board Members.