USALI Perspectives

Volume 1, Number 18
Published April 1, 2021

Understanding China's Growing Influence in Global Data Governance

Looking beyond US-China relations

By Matthew S. Erie & Thomas Streinz

The Trump Administration's moves to ban the Chinese-owned apps TikTok and WeChat in the United States out of concerns that the data of U.S. citizens could be shared with the Chinese government have been extensively discussed. What is less debated—or, for that matter, even understood—is China's influence on data governance *globally*, particularly in developing countries. China's impact is likely to be more significant in emerging economies where Chinese tech companies are supplying information and communications technology, e-commerce platforms, and digital surveillance technology, than in the US or European Union.

Our forthcoming article, "The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance," explains, through an interdisciplinary and empirical account, based on research conducted over a four-year period, how Chinese tech companies, their reception by the domestic law and politics of host states, and China's involvement in institutions of global governance and international law are shaping data governance globally.

By "transnational data governance," we mean the rules, norms, practices, and infrastructures governing the collection, storage, transfer, use of, and access to data across national borders. A prevailing explanation for the transnational effects of one jurisdiction's data governance regime is Anu Bradford's *Brussels Effect*. Bradford posits that the EU's General Data Protection Regulation or GDPR is emulated beyond the EU because multinational corporations gravitate towards it. However, China's impact on data governance, and on global governance more generally, operates through different mechanisms. One of the most significant of these is Chinese enterprises' supply of digital infrastructure in host states.

Beijing claims that its "Digital Silk Road" is promoting "unlimited" transnational digital development through the cross-border supply of digital infrastructure by Chinese companies. Critics of "digital authoritarianism" suggest that Beijing is exporting its values along with its technology to nondemocratic states. We suggest a more nuanced explanation of such dynamics, which we shorthand as the "Beijing Effect." The "Beijing Effect" theorizes that China influences data governance outside China through a complex combination of "push" and "pull" factors.

On the push side, the Chinese government promotes the concept of "data sovereignty" as a justification for its approach to data governance. China has consistently argued for "cyber sovereignty" in various international institutions, ranging from the UN's intergovernmental working groups on international law in cyberspace to multi-stakeholder Internet

governance institutions such as ICANN. The push for "data sovereignty" continues this agenda by asserting governmental control over in-country and transnational data flows. China has also spearheaded its own initiatives such as the World Internet Conference and the Global Data Security Initiative. In November 2020, China joined the Regional Comprehensive Economic Partnership, which permits restrictive data policies when member states deem them necessary.

On the pull side, many developing countries exhibit strong demand for Chinese investment in digital infrastructures, especially along the "Belt and Road Initiative." These infrastructures include fiber-optic cables, data centers, satellite networks, surveillance technology for so-called "safe" or "smart" cities, and e-commerce and communications platforms. These infrastructures are built, operated, and maintained by Chinese companies, including Alibaba, Huawei, ZTE, Jingdong, and Chinese telecoms – all companies that are subject to the formal law of the People's Republic of China and, to varying degrees, operate under the influence of the Chinese Communist Party.

Potential conflict of laws between a company's home and host state is not unique to China. Similar issues may apply to the U.S. Cloud Act and the EU's GDPR. What is different about the Beijing Effect is the entanglement of Chinese companies with the Party-State. The Chinese version of data sovereignty – in contrast to European aspirations under the same label – combines governmental control over domestic and cross-border data flows with an increasingly assertive authoritarian regime.

> *Many states – not only authoritarian ones – seek some version of data sovereignty to control access to and transfer of data.*

Why are host states increasingly relying on digital infrastructure supplied by Chinese tech companies? The straightforward answer is that some Chinese technology is both relatively cheap and high quality. But there is a more fundamental appeal, namely, the twin aspirations of data sovereignty and digital development that are attractive to governments in developing economies. Many states – not only authoritarian ones – seek some version of data sovereignty to control access to and transfer of data. This driver may cause them to emulate certain aspects of PRC data law. An example is Vietnam's borrowing from the 2017 PRC Cybersecurity Law. China has made a strong case for digital development through data-driven innovation, accessible digital infrastructure, and e-commerce, as recognized, for example, by the World Bank. China's rapid transition towards a digitally-mediated economy and society complicates the conventional narrative that governmental control over data flows necessarily jeopardizes the economic and social benefits of digital development.

One consequence of the Beijing Effect is the mutual learning that occurs between host states and Chinese enterprises when developing digital infrastructure projects. A concrete example is the installation of Huawei's facial recognition cameras in Brazilian cities, for instance, in Campinas, a major city in the state of São Paulo. An open question is whether this surveillance technology complies with Brazil's nascent data protection law. The *Lei Geral de Proteção de Dados*, which resembles core aspects of the EU's GDPR, formally entered into force in September 2020, but independent data protection authorities were only established months later. Nevertheless, already in February 2020, a local court from São Paulo suspended a public announcement for the installation of facial

recognition cameras in the city's metro, for which Huawei was expected to make a bid, citing data protection concerns under the future law. In March 2021, São Paulo's governor vetoed a state bill that would have allowed the installation of facial recognition cameras to go forward. These episodes illustrate how Brazil's data protection regime is evolving, and Chinese companies will have to adapt.

Brazil is not the only example of Chinese tech companies experiencing a learning curve. The Indian government recently upheld its Ministry of Electronics and Information Technology's ban on 59 Chinese apps, including TikTok, WeChat, and Alibaba's UC Browser, citing privacy and compliance concerns. TikTok has faced bans in Muslim-majority Asian countries, including Indonesia, Bangladesh, and Pakistan, based on arguments that its content was "un-Islamic" and incongruent with the values of the host state. These examples show that whereas it is often assumed that China is hegemonic and host states powerless, such characterizations fail on empirical grounds. Local regulatory frameworks may impose costs on Chinese tech companies, even if such frameworks are nascent.

Insights from empirical legal studies and a more comprehensive understanding of data governance, which is attentive to the various ways in which law and infrastructure regulate data, can shed light on how the complex interaction among Chinese authorities, Chinese tech companies, and different developing countries affects data governance domestically and globally.

***

Matthew S. Erie *is associate professor of Modern Chinese Studies and associate research fellow of the Socio-Legal Studies Centre at the University of Oxford;*

Thomas Streinz *is executive director of Guarini Global Law & Tech, adjunct professor at NYU School of Law, and a fellow at the Institute for International Law and Justice*
