INTERNATIONAL ENCRYPTION BRIEF

MARCH 2021

The Encryption Debate in China: 2021 Update

Lorand Laskai and Adam Segal

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Chinese encryption policy is shaped by two competing interests—political control and commercial development. Beijing requires commercial companies maintain backdoors or key escrows to preserve government access to data for public security and intelligence gathering, which has discouraged the widespread adoption of commercial encryption. It has also long demanded the encryption industry prioritized the development of "secure and controllable" encryption, which has impeded the industry's growth. At the same time, Chinese officials increasingly see encryption as integral to developing China's digital economy, particularly blockchain technologies, and to redress growing awareness among Chinese users about the vulnerability of their personal data. While Beijing's emphasis on control continues to motivate the country's policies, the country's new Encryption Law has unexpectedly liberalized restrictions on encryption technology—suggesting policymakers are willing to prioritize digital economic development, at least for the moment.

This shift has come as the U.S.-China trade war morphs into a larger technological struggle that has pitted China techno-nationalist ambitions against U.S. control of critical technology. The 2019 blacklisting of Huawei signaled a new willingness in Washington to restrict the supply of critical components to curb China's indigenization efforts, especially semiconductor manufacturing equipment and semiconductor electronic automation design tools. In response, China has doubled down on its goal of "self-developed, controllable" ICT supply chains. The Fourteenth Five Year Plan (2021–2025) focuses on a "dual circulation" strategy that emphasizes domestic innovation and technological autonomy along with a growth in domestic consumption.

These efforts, of course, are not new—and encryption has a long history of being a test bed and early focus of Chinese efforts at indigenization. In the past, foreign governments and firms complained about the use of domestic standards and certifications designed with the goal of bolstering the competitiveness of domestic companies. Through the Multi-Level Protection Scheme, for example, Chinese authorities created mandatory domestic intellectual property requirements in specific sectors. In addition, agencies pushed for the mandatory adoption of WAPI, ZUC, and other encryption standards by foreign firms in an effort to encourage broader use of Chinese encryption standards.

Yet, amid this backdrop, China's recent handling of encryption has bucked the trend of indigenous innovation. Rather than tightening its grasp on encryption as a tool of a techno-nationalist agenda, Beijing has considerably liberalized the use of commercial cryptography, easing restrictions on foreign firms and loosening regulation on commercial encryption. In addition, in the face of an increasingly ever-present surveillance state, which has further expanded and scaled as the government moved to monitor the development and transmission of COVID-19, Chinese officials appear poised to require companies to encrypt certain types of sensitive data like personal information and financial transactions—which could make government access and monitoring more difficult.[1]

The cornerstone of this push toward liberalization of commercial cryptography standards and uses is China's Encryption Law, which went into effect in January 2020.[2] As the country's first law comprehensively regulating encryption technologies, products, and services, the Encryption Law replaced a two-decade-old patchwork of encryption regulation that excluded foreign encryption and strictly regulated all encryption products developed, used, and sold in China as state secrets. This regulatory regime constituted the basis of an exclusionary industrial policy intended to keep foreign companies at bay as China built out domestic alternatives. The government complemented the regulatory efforts with centrally guided initiatives to get domestic encryption standards accepted as international standards—a push that created several misfired and middling successes.

At least initially, even before they saw any wording, multinational companies and external observers expected the Encryption Law to further exclude foreign encryption. China's emerging cybersecurity regime has largely cut foreign companies out of the policy formulation process, reducing their influence and often saddling them with regulation that disadvantages them against domestic rivals. Once released, the initial draft offered reason for concern. It made no reference to the "secondary function" exception that had allowed foreign software and technology in which encryption is not the core function to continue operating in China.

However, to the surprise of many, the adopted Encryption Law relaxed control over commercial encryption, significantly recalibrating previous controls in the favor of openness. Unlike the previous encryption regime, the Encryption Law aims to foster a domestic industry with foreign participation and to encourage the domestic adoption of encryption. The law carves out commercial encryption from encryption used to protect state secrets or secure critical information infrastructure, relaxing many of the requirements placed on the former, including mandatory inspection and testing.[3] Most significantly, this carve out means that foreign firms can enter the market and sell their encryption products for the first time. Reinforcing these moves toward openness is language in the law instructing officials to "follow the principle of non-discrimination" and encourage cooperation and foreign investment.[4]

Behind this liberalization of one of China's most restricted technology sectors appears to be a strategic calculation that state-led development and exclusionary industrial policies had lost their utility in commercial encryption. Chinese officials now see a greater role for encryption in supporting the future development and security of China's digital economy. The country's State Cryptography Administration has, for example, hailed encryption as a "strategic resource."[5] The country's senior leadership not only wants to bolster the trustworthiness of Chinese digital products in export markets, it also has taken an interest in harnessing blockchain technology, going so far as to hold a Politburo session last year specifically to study the technology.[6] The country still trails in developing cutting-edge encryption technologies required for emerging applications, including blockchain and

quantum proof cryptography. Further development in these cutting-edge applications, Chinese officials believe, will require openness to foreign collaboration and competition. China cannot be a leader in blockchain without a world-class encryption industry—something the country currently lacks. In short, Beijing will need both competitive domestic firms and foreign technology players.

There also appears to be a consensus among some officials that over-regulating encryption has hampered the adoption of encryption as a matter of basic cybersecurity.[7] In this regard, reducing regulation should stimulate the industry and drive adoption. Officials appear ready to reinforce this with new data protection regulations requiring companies to encrypt certain types of data and communication. A draft of China's Data Security Law, which was posted for public comment in August 2020, included provisions for mandatory data security standards, and some preliminary guidance measures suggest that companies handling sensitive data will need to encrypt their data.[8]

Despite the moves in favor of liberalization and greater adoption of encryption, the emerging regulatory framework does allow officials room to maneuver, and there could be backsliding in the future. For one, there are significant ambiguities in the Encryption Law and how it interacts with China's existing regulatory architecture for cybersecurity to allow officials to maintain the exclusionary practices of the past if they so wish. For example, while foreign encryption makers can now enter China's commercial encryption market, commercial encryption that involves "national security or the societal public interest" requires an import permit; the vague language of this exception could be used to in effect exclude firms from a broad swath of the market.[9]

Similar ambiguities persist for internet operators, many of which should at least on paper have greater latitude in how they encrypt their services. However, operators could fall within one of two heightened security schemes—one for critical information infrastructure and another, the Multi-Level Protection Scheme, for companies handling sensitive information. Both schemes require national security reviews for encryption, and conspicuously, neither scheme has a clearly centrally defined scope. While the Cyberspace Administration of China issued a draft Critical Information Infrastructure regulation in 2017, it still has not finalized it. This means that companies, if in doubt about their status, will err on the side of caution and buy encrypted products from domestic firms that have passed all requisite security processes.

Second, companies will still need to abide by government requests for access to data even as the country's cyber regulators inch toward mandating encryption sensitive data and communication. Categories of data likely to eventually require encryption include financial transactions, biometrics features, geolocation history, and forms of personal information like race, ethnicity, and medical history.[10] These happen to be categories of data that the government is also interested in collecting for surveillance and stability maintenance.[11] While the Encryption Law does not contain an explicit

provision requiring companies to decrypt data for security and intelligence gathering purposes, the Cybersecurity Law established a legal obligation for internet operators to turn over data upon request.[12] This obligation is further reinforced in the draft Data Security Law released in August 2020. This points to a fundamental reality of data governance in the Chinese market: while the Chinese government is working to protect users against cyber criminals, individuals and businesses can have no expectation of the security of their data against the state.

The liberalization of encryption policy comes with the caveat that the government must have the key. Beijing wants to encourage development of encryption capabilities to defend Chinese data and communications from criminal and foreign actors, while ensuring that the Chinese government has keys to decrypt everything for its own use. To foster development of domestic capabilities, which still lag behind Western standards, Chinese officials want to encourage foreign innovators and businesses to operate in China or cooperate with Chinese counterparts. However, it remains to be seen how the Chinese government's insistence on holding the keys will limit foreign counterparts' interest in collaborating and whether that will slow domestic development.

About the Authors

Lorand Laskai is a JD candidate at Yale Law School. He was previously a research associate at the Council on Foreign Relations.

Adam Segal is the Ira A. Lipman chair in emerging technologies and national security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations.

About the Encryption Working Group

The Carnegie Endowment for International Peace and Princeton University have convened a small group of experts to advance a more constructive dialogue on encryption policy. The working group consists of former government officials, business representatives, privacy and civil rights advocates, law enforcement experts, and computer scientists. Observers from U.S. federal government agencies attended a select number of working group sessions. Since 2018, the working group has met to discuss a number of important issues related to encryption policy, including how the relevant technologies and uses of encryption will evolve in the future.

This briefing paper and its companion pieces detailing the encryption debates in a select number of key countries and regions—Australia, Brazil, China, the European Union, Germany, and India—were prepared by local and area experts at the request of the Encryption Working Group. They are designed to shine light on key drivers of the debates in these countries, how they have evolved in the last five years, and the divergent approaches taken by different governments. The briefs do not take a position on encryption policy, rather they provide analysis of how debates about encryption have evolved internationally. The views are the authors' own and do not necessarily reflect the views of Carnegie or the Encryption Working Group.

Notes

1 Emily Feng, "In China, A New Call To Protect Data Privacy," NPR, January 5, 2020, https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy.

2 "中华人民共和国密码法" [Encryption Law of the People's Republic of China], National People's Congress of the People's Republic of China, October 26, 2019, http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

3 Ibid, chapter 3.

4 Ibid, article 21.

5 "中华人民共和国密码法》发布 这六个问题你需要知道" [The PRC's Encryption Law: The Answers to Six Questions You Should Know"], *People's Daily*, hosted by Cyberspace Administration of China, October, 29, 2019, http://www.cac.gov.cn/2019-10/29/c_1573880702680488.htm; Nicole Lindsey, "China's New Encryption Law Highlights Cryptography as a Strategic Priority," CPO Magazine, November 11, 2019, https://www.cpomagazine.com/data-protection/chinas-new-encryption-law-highlights-cryptography-as-a-strategic-priority/.

6 Liu Zhen, "Chinese President Xi Jinping Calls for More Research, Investment Into Blockchain Technology," *South China Morning Post*, October 26, 2019, https://www.scmp.com/news/china/diplomacy/article/3034716/chinese-president-xi-jinping-calls-more-research-investment.

7 The authors thank Samm Sacks for making this point.

8 See for example, "《天津市数据交易管理暂行方法（征求意见稿）》公开征求意见" [Tianjin Municipal Government, Interim Measures for the Administration of Data Transactions (Draft for Solicitation of Public Comments)], Sina Tianjin, July 31, 2020, http://tj.sina.com.cn/news/zhzx/2020-07-31/detail-iivhuipn6009892.shtml.

9 "Encryption Law of the People's Republic of China," article 28.

10 Sensitive personal information" is an evolving category in China. The latest draft of the forthcoming Personal Information Protection Law provides the current range of data covered in article 28. See Rogier Creemers, et al, "China's Draft 'Personal Information Protection Law' (Full Translation)," New America, October 21, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-draft-personal-information-protection-law-full-translation/.

11 For an overview of Chinese domestic surveillance initiatives, including what forms of data Chinese officials have sought access to, see Dahlia Peterson, "Designing Alternatives to China's Repressive Surveillance State," Center for Security and Emerging Technology, October 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Designing-Alternatives-to-Chinas-Surveillance-State.pdf.

12 Emma Rafaelof, et al., "Translation: China's 'Data Security Law (Draft)'," New America, July 2, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

1779 Massachusetts Avenue NW | Washington, DC 20036 | P: + 1 202 483 7600

CarnegieEndowment.org