INTERNATIONAL ENCRYPTION BRIEF

MAY 2019

The Encryption Debate in China

Lorand Laskai and Adam Segal

The Encryption Debate in China

Lorand Laskai and Adam Segal

For your convenience, this document contains hyperlinked source notes as indicated by teal colored text.

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.

CONTENTS

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.

The Encryption Working Group will continue its efforts to study this important issue and plans on releasing further briefings on aspects of the encryption policy debate.

Members of the Encryption Working Group include:

Jim Baker
Former General Counsel, Federal Bureau of Investigation

Katherine Charlet
Program Director, Technology and International Affairs, Carnegie Endowment for International Peace

Tom Donahue
Visiting Fellow, George Mason National Security Institute, and former Senior Director for Cyber Operations, National Security Council, White House

Ed Felten
Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University

Avril Haines
Senior Research Scholar at Columbia University's Columbia World Projects and former Deputy Director, Central Intelligence Agency

Susan Hennessey
Executive Editor, Lawfare, and Senior Fellow in Governance Studies, the Brookings Institution

Chris Inglis
Managing Director, Paladin Capital Group, and former Deputy Director, National Security Agency

Sean Joyce
US Cybersecurity and Privacy Leader, PwC, and former Deputy Director, Federal Bureau of Investigation

Susan Landau
Bridge Professor of Cyber Security and Policy, Tufts University

Christy Lopez
Distinguished Visitor from Practice, Georgetown Law Center

Alex Macgillivray
Board Member, Data & Society, and former Deputy Chief Technology Officer of the United States

Jason Matheny
Founding Director, Georgetown Center for Security and Emerging Technology, and former Director, Intelligence Advanced Research Projects Activity

Tim Maurer
Co-Director and Fellow, Cyber Policy Initiative, Carnegie Endowment for International Peace

Denis McDonough
Visiting Senior Fellow, Technology and International Affairs, Carnegie Endowment for International Peace, and former White House Chief of Staff

Lisa Monaco
Distinguished Senior Fellow, Reiss Center on Law and Security, New York University School of Law, and former Assistant to the President for Homeland Security and Counterterrorism

Laura Moy
Executive Director, Center on Privacy & Technology, Georgetown Law Center

Michelle Richardson
Director, Privacy and Data Project, Center for Democracy and Technology

Ronald L. Rivest
Institute Professor, Massachusetts Institute of Technology

Ari Schwartz
Managing Director of Cybersecurity Services, Venable LLP

Harlan Yu
Executive Director, Upturn

Denise Zheng
Senior Associate (Non-resident), Technology Policy Program, Center for Strategic and International Studies

Note: This is not a comprehensive list of all members. Some wish to remain anonymous for the time being and to contribute in their personal capacity.

The encryption debate in China has historically been driven by the goals of economic development, technological autonomy, and national security. Starting in the late 1990s, encryption became one tool in a larger set of industry policies designed to bolster the competitiveness of domestic IT firms. These policies, including the use of domestic standards and certifications, pit the Chinese government against foreign governments and multinational IT vendors. In addition, Chinese leaders have real concerns about the vulnerabilities that come from dependence on foreign suppliers. As China has grown into a technological power, the encryption debate has expanded to concerns about individual users, and the tension between government access and personal information protection in particular. Moving forward, the encryption debate will be shaped by bureaucratic politics; by the interaction of Beijing and foreign firms; and by the growing demands for personal security from Chinese users and the national security demands of the Chinese government.

Introduction

While the debate surrounding encryption in the United States and Europe has centered on privacy and law enforcement access, the encryption debate in China historically has been driven by the goals of economic development, technological autonomy, and national security. Starting in the late 1990s, encryption became one tool in a larger set of industrial policies designed to bolster the competitiveness of domestic information technology (IT) firms. These policies, including the use of domestic standards and certifications, pit the Chinese government against foreign governments and multinational IT vendors like Microsoft, IBM, and Cisco.

In addition to these economic motivations, Chinese leaders have real concerns about the vulnerabilities that come from dependence on foreign suppliers. The Edward Snowden revelations in 2013 confirmed what many in China already believed: that dependence on U.S. IT vendors left China's network infrastructure vulnerable to eavesdropping. The revelations reenergized preexisting efforts to promote "secure and controllable" technology and encourage its adoption in sensitive sectors to guard against foreign spying. In 2014, President Xi Jinping formed the Leading Small Group on Cybersecurity and Informatization, a high-level body tasked with overseeing issues related to the digital economy and cyber defenses. Under the mantra of "without cybersecurity, there is no national security," the central leadership jumpstarted efforts to localize data and build out a domestic technical standard-setting regime.

As China has grown into a technological power—by some accounts, it is now the second largest digital economy in the world—the encryption debate has encompassed concerns about individual users. China now has more than 800 million internet users and more than 1.5 billion cell phone subscriptions, and the tension between government access and personal information protection constitutes an increasingly large part of China's evolving encryption debate. On one hand, the Chinese government has set out a legal obligation for tech companies to provide access to data for public security and intelligence gathering purposes. This has meant that Chinese tech companies either eschew certain types of encryption or they utilize encryption on commercial products with a backdoor or key escrow. On the other hand, poor cyber hygiene and rampant cyber crime have

sparked rising awareness of privacy and a demand for personal information security among Chinese citizens.

A burgeoning black market for personal data has led regulators to impose obligations on tech companies to secure sensitive personal data through encryption. However, a countervailing obligation to guarantee public security officials access to user data is likely to influence how platforms store data. Notably, no major Chinese app utilizes end-to-end encryption, which has become the industry standard among international messaging platforms like WhatsApp, Telegram, and iMessage. In addition, China's push for big data policing ensures that authorities will want access to a wide range of data. Initiatives like the nascent social credit system, which over time could marshal disparate streams of personal data to score the perceived trustworthiness of citizens, will likely create an impetus for tech companies to store as much user data as possible.

Key Actors

Very little of China's encryption debate occurs in public. Much of the existing public discourse involves the Chinese media covering encryption debates in other counties primarily as a way to justify the policies that China is pursuing**.** For instance, the Chinese press has drawn comparisons between the decryption provision in China's Cybersecurity Law and Australia's 2018 encryption law and the United Kingdom's 2016 surveillance law. Similarly, in March 2015, in response to U.S. criticism of draft provisions in China's Counterterrorism Law that appeared to require the installation of backdoors and the reporting of encryption keys, Chinese Ministry of Foreign Affairs spokesperson Lu Kang responded, "If you do some research, you will find no difference between the provision and relevant legislation by western countries. I believe double standards have no place to play on this issue."

The majority of what might be considered the encryption debate in China appears to occur through governmental consultation with domestic actors and, occasionally, foreign actors. The primary central government agency tasked with regulating encryption is the Office of State Commercial Cryptography Administration (OSCCA), or the Guojia Shangyong Mima Guanli Bangongshi, sometimes alternatively called the State Cryptography Administration (SCA), or the Guojia Mima Guanliju. This agency was established in 2005 and falls under both the Chinese Communist Party General Office and the State Council. It is the administrative office of the Central Leading Small Group on Encryption.

The OSCCA plays a prominent role in a broader, more complex regulatory ecosystem. It consults and jointly releases regulations and guidance with other state organs, including the Ministry of Public Security (MPS), the State Secrecy Bureau, and the State Council Information Office. The Cyberspace Administration of China (CAC) plays a role in developing a cybersecurity review regime for network equipment as part of the Cybersecurity Law, though the law mentions encryption only once, calling

for carriers to use a procurement framework called the Multi-Level Protection Scheme (MLPS) and include encryption. Various other regulators and ministries have released drafts of industry-specific implementation guidelines; for example, the People's Bank of China and the Ministry of Education have released guidelines for the finance and education sectors, respectively. Every province and provincial-level city also have their own cryptography administrations, which publicize, oversee, and enforce central decisions in their given jurisdictions.

Beyond its aforementioned functions, the OSCCA includes a cryptography research institute, an encryption analysis and testing center, and a dedicated chip laboratory (for secure cryptoprocessors). It also organizes industry conferences and oversees efforts to create and promote encryption standards in cooperation with China's Standardization Administration through the Encryption Industry Standardized Technology Committee (or the Mima Biaozhun Weiyuanhui). A large part of the committee's work seems to be releasing indigenous encryption standards.[1] The encryption practices used for military and party documents and communications are handled by separate systems and suppliers, on which there is very little public reporting.[2]

A few other state organs also bear mentioning. The Chinese Association for Cryptologic Research (CACR), or the Zhongguo Mima Xuehui, was established in 2007 to promote cryptographic research. The association currently has about 2,980 individual members and 158 organizational members; it publishes a bimonthly journal and hosts conferences on cryptography. The National Information Security Standardization Technical Committee, or the Quanguo Xinxi Anquan Biaozhunhua Jishu Weiyuanhui, plays an important role in setting technical standards. Over the past several years, the committee has put out nearly 300 national cybersecurity standards, including several related to encryption. Most of these standards are not mandatory, but their adoption may be required for certain sectors under the MLPS or the Cybersecurity Law. While international companies are represented on a number of subcommittees that set standards, the encryption working group (Working Group 3) does not accept foreign members and has a clear bias toward domestic cryptography and encryption.

Main Issues

Early Attempts at Regulation

Beijing's early forays into regulating encryption included some concessions in the face of international pushback but maintained strong government control of the direction of policy and the development of encryption technology. The Chinese government's first attempt at such regulation occurred in 1999 with the release of Directive No. 273, which effectively banned foreign encryption products and imposed a stringent restriction on all encryption products. As originally written, the directive specifically mandated that all encryption produced, distributed, and sold in China must

receive approval from the newly established OSCCA. In addition, the regulation empowered OSCCA to inspect companies' IT, including proprietary source code.

The directive immediately triggered an outcry from foreign companies and governments. Companies including Microsoft expressed concerns that the regulation would be used to facilitate intellectual property theft and cut foreign IT companies out of the Chinese market. Under pressure, Chinese officials quickly walked back the regulation. In a clarifying document issued in March 2000, they revealed that only hardware and software using encryption as "core functions" would be regulated under the law. With this change, products in which encryption was a "secondary function" (such as laptop computers, mobile phones, web browsers, and software) fell outside the directive's purview.

The capitulation likely indicated a lack of internal consensus within the Chinese government on encryption technologies, at least with respect to implicit goals in the directive. As Shazeda Ahmed and Steven Weber argue, the fact that the directive regulated the use of encryption in the commercial sector and not government ministries suggests that economic concerns overrode security concerns as the regulation was being formulated. At the time, foreign IT vendors like Microsoft, IBM, Intel, and Cisco dominated the Chinese IT market, and the Chinese government had clear aims to expand the market share of domestic companies.

While the 2000 clarification looked like a retreat on the part of the Chinese government, it still left in place important components of the original directive, including the review and approval process for products in which encryption is the primary function. In 2005, the OSCCA fined Hewlett-Packard for selling personal laptops loaded with an unapproved security chip. Moreover, the directive marked the beginning of a series of pushes and pulls between Beijing and foreign companies over China's attempts to use encryption technology as an exclusionary industrial policy over the next two decades.

To illustrate, China's first major foray into standard-setting for encryption was the WLAN Authentication and Privacy Infrastructure (WAPI) standard.[3] Claiming that WAPI was more secure than the prevailing standard of the U.S.-based Institute of Electrical and Electronics Engineers (IEEE), 802.11 WiFi, the Chinese government in 2003 mandated that all wireless devices sold in China must run WAPI. The government justified the decision based on national security concerns, although the government-approved vendors that could license the WAPI standard stood to gain considerably from licensing and royalty fees.

According to the mandate, foreign IT vendors would need to work with an approved Chinese vendor to install WAPI-enabled equipment, an arrangement that would expose foreign intellectual property to potential theft. Intel pushed back against the new regulation, going so far as to announce that it would stop shipments of the Centrino WiFi chip, which at the time was used in half of all laptops in China, according to one estimate. China ultimately scrapped the regulation, but only after

the U.S. government threatened to pursue a case at the World Trade Organization (WTO) and the International Organization for Standardization rejected the standard.

The demise of the government mandate that WAPI be used stoked resentment among many Chinese technologists. The China Broadband Wireless IP Standards Working Group, which created the WAPI standard, accused the IEEE of engaging in "cultural chauvinism" and "trying to destroy WAPI by every means." Despite these setbacks, Apple and Dell both eventually introduced phone models that supported WiFi and WAPI, a sign of the Chinese government's successful ability to leverage market access to shape the behavior of foreign companies.

In 2011, the OSCCA mandated ZUC, a stream cipher–based encryption algorithm developed by the Chinese Academy of Sciences for 4G Long-Term Evolution (LTE) equipment. Unlike WAPI, ZUC enjoyed success in international standard-setting bodies. The European Telecommunications Standards Institute approved it in 2011, and the standards organization known as the Third Generation Partnership Project adopted it as a voluntary standard. Because it is the largest cell phone market in the world, if China had chosen to mandate the adoption of ZUC, that would have incentivized telecommunications companies to adopt it elsewhere.[4] After another round of international pushback, China agreed at the 2013 meeting of the U.S.-China Joint Commission on Commerce and Trade to not demand compliance with the ZUC standard as a precondition for selling in its domestic market.

Sector-Specific Domestic Technology Mandates

Even though the attempted mandatory adoption of specific encryption standards has been largely unsuccessful at encouraging other parties to adopt Chinese encryption standards, Chinese authorities have had greater success at creating mandatory domestic intellectual property requirements in specific sectors. In 2007, the MPS released the MLPS procurement framework, which requires that critical infrastructure and high-risk sectors use domestic IT, including domestic encryption technology. The MLPS laid out a grading system that ranks the security of network applications based on the risk they pose to national security, the public interest, and social stability: level one denotes little impact, whereas level five indicates an "especially grave" impact.

Under the MLPS, operators of systems classified as level three or above are required to use indigenous technology for core systems and undergo a certification process. For encryption standards, compliance at level three and above requires the use of Chinese encryption algorithms. The systems classified at level three and above encompass a broad swath of commercial sectors including banking, finance, communications, commerce, healthcare, and education. The Information Technology Industry Council posited that roughly $35 to $40 billion of the nearly $60 billion China spent on commercial and public sector IT in 2010 fell under the terms of the MLPS.

The OSCCA has a range of tools at its disposal to enforce the MLPS. These include unannounced inspection visits, access to encryption keys or cryptologic protocols, and the power to request that companies hand over source code for inspection. While MLPS enforcement has been uneven, many domestic and foreign companies have complied anyway to avoid disruption of service.

In the aftermath of the Snowden revelations, China doubled down on the requirement that sensitive sectors use domestic intellectual property. The 2017 Cybersecurity Law established a separate regulatory regime for network operators, overseen by the CAC. Under the law, operators of "critical information infrastructure" (CII) can only use network equipment and cybersecurity products that are approved by designated bodies. The new security review will likely entail scrutinizing cryptographic source code.

However, in the nearly two years since the Cybersecurity Law went into effect, critical details about the law, including which sectors are classified as CII, remain unanswered. In July 2017, the CAC published a draft of the CII Security Protection Regulations for public comment, but a finalized version of the regulation has not yet materialized. In addition, despite their overlapping scopes of authority, the CAC and the MPS have yet to clarify how the law's CII provision relates to the MLPS procurement framework.

On top of the uncertainty regarding the Cybersecurity Law, the OSCCA released an April 2017 draft of a new Encryption Law, which would comprehensively overhaul how the Chinese government regulates encryption. Under the law, encryption will fall into three categories: "core encryption," "common encryption," and "commercial encryption." Data that is defined as a state secret must be stored using core or common encryption; everything else uses commercial encryption. The draft does not clarify the difference between core and commercial encryption, nor does it explicitly say whether the secondary function exception that foreign companies have relied on since Directive No. 273 was promulgated will remain in place under the new law.

A Deep Dive

Nearly two decades after Directive No. 273 was formulated, China's encryption regulatory regime remains a product of the government's diverging goals. Early attempts at regulation like Directive No. 273 and the WAPI standard mandate appear to have been mainly motivated by economic development goals. While better security may have been found in foreign products, given the immaturity of the country's domestic producers, economic goals often overrode the security concerns of users and specialized ministries in those early years. The MLPS and especially the 2013 Snowden revelations then shifted the pendulum toward greater Chinese concern about the vulnerabilities that come from dependence on foreign suppliers. Throughout this period, strong opposition from international tech companies and foreign governments led the Chinese state to roll back or slow-walk the implementation of regulations.

The result has been an incomplete Chinese regulatory system for encryption. There are some indications that existing and future regulations will converge around the CII provision of the Cybersecurity Law. The MPS is currently revising the MLPS, which will bring it under the jurisdiction of the CAC. This means that the new iteration of the procurement framework (MLPS 2.0) will likely be harmonized with the scope of the CII provision. Similarly, the draft of the Encryption Law stipulates that the OSCCA will conduct a security review of encryption used by CII operators. The CII provision clearly constitutes the keystone of China's evolving encryption regulatory regime.

Yet the criteria for designating CII operators remain in flux, and Beijing is under international pressure to define the scope of CII narrowly. According to the *Wall Street Journal*, as a potential concession in the talks to end the U.S.-China trade war, Chinese negotiators have floated the idea of defining CII operators based on market share rather than sector, a definition that would considerably narrow the provision's scope.

Even as China's regulatory approach to encryption slowly takes shape, the ground under this ongoing debate is shifting, given that Chinese citizens' views about how their data is used and protected are taking on added salience. The concerns of individual users are gradually taking center stage, and the Chinese government is placing the onus on tech companies to better secure user data. To date, personal data protection standards in China have not kept pace with the growing importance of digital technologies in everyday life. A September 2018 survey found that more than 80 percent of participants reported being victims of data leaks in one form or another. Much of this data often ends up on the thriving black market. One 2017 exposé by two Chinese journalists captured the scope of the challenge, reporting that, for a modest fee, they were able to acquire a wide array of personal information on colleagues—from hotel check-in history, apartment rentals, bank deposit records, and even live location-tracking data.

In May 2018, China's first comprehensive standard for data protection, the Personal Information Security Specification, went into effect. It outlines best practices for the collection, use, transfer, and storage of personal data. In cases of data transfer and storage, the specification explicitly requires that companies use security techniques like encryption. The Chinese government is employing a range of means to induce corporate compliance with what is ultimately a nonbinding standard, including by making references to violations of the specification during audits and investigations. The specification also will likely provide the basis for the Personal Information Protection Law, which is on the 2019 legislative agenda of the National People's Congress.

Some Chinese companies have begun introducing products with more privacy features in response to these consumer concerns over data protection and privacy. Huawei has advertised the file-based encryption function on its flagship smartphone, the Mate 9. In a digital ad campaign, the Chinese smartphone maker Gionee emphasized the security features of its M6S Plus model, including a

secure cryptoprocessor. Some Chinese entrepreneurs like Yang Geng, the former chief security officer at Amazon China and Xiaomi, have launched start-ups related to privacy and encrypted services.

But it is unclear how far the Chinese government will allow companies to go when it comes to encrypting commercial services. Since the 2015 Counterterrorism Law took effect, the Chinese government has gradually outlined a legal obligation for tech companies to provide technical and decryption assistance for public security and intelligence gathering purposes. The 2017 National Intelligence Law further solidifies that obligation, as does the Cybersecurity Law, which requires tech companies to store internet logs of users' online activity for at least six months to aid law enforcement. Insofar as encryption makes accessing user data more difficult, these laws are likely to deter companies from fully embracing encryption.

These legal provisions even seem to be affecting the operational decisions of foreign companies. In response to the Cybersecurity Law, Apple announced in January 2018 that it would migrate iCloud data for Chinese users to a domestic cloud service provider run by Guizhou-Cloud Big Data, a division of China Telecom. The decision seems to have been motivated in part by joint venture requirements and the data localization provision in the Cybersecurity Law, but it appears that the legal obligation to assist Chinese authorities also played a role: Apple later clarified that it would also transfer the encryption keys for Chinese iCloud accounts to China. This move is likely to streamline the process of providing user data to Chinese authorities upon request, though some have questioned whether Apple's joint venture partner can act unilaterally if such requests are made.

Notably, unlike major international communications apps like WhatsApp, Facebook Messenger, iMessage, or Telegram, no major domestic Chinese messaging platform has adopted end-to-end encryption, likely because such encryption would make a considerable amount of user data inaccessible to platform operators. Chinese authorities have made their disapproval of end-to-end encryption known, banning two encrypted South Korean messaging apps, Line and Kakao Talk, in 2014. In September 2017, Chinese censors finally blocked WhatsApp, the last Facebook product available in China and the last major end-to-end encryption messaging service in China aside from iMessage.[5]

While multinational firms have traditionally had limited influence on China's domestic encryption debate, there have been a few instances in which foreign pressure has shaped policy outcomes, such as the eventual decision to discard the WAPI mandate. An early draft of the Counterterrorism Law, for example, stipulated that "telecommunications service providers" and "internet service providers" must disclose their encryption practices to the Chinese government and provide the government with the technical means to continue accessing information on the network. The final provision, after foreign protests, contained a less specific requirement to "provide technical support and assistance, such as technical interface and decryption, to support the activities of the public security and state security authorities in preventing and investigating terrorist activities." Foreign firms also

had success in suspending banking regulations that would have required banks to allow Chinese regulators to examine their encryption algorithms.

Outlook

Moving forward, the encryption debate in China will be shaped by a series of factors, including domestic bureaucratic politics; interactions between Beijing and foreign firms; and the interplay between Chinese users' growing demands for personal security and the Chinese government's national security demands.

The outcomes of the first two are easier to predict. In bureaucratic terms, despite the high-level attention to cybersecurity and encryption policy, the Chinese policy process will continue to be incremental and incomplete. No single agency will have unquestioned authority as various actors, as well as the central government and local authorities, bargain over jurisdiction and influence.

Meanwhile, foreign companies are likely to get results at the margins of Chinese encryption policy. Foreign analysts expect that the final form of the Encryption Law will reduce the regulatory burden for using encrypted products in China—a development that foreign companies will welcome. A September 2017 State Council decision to remove the approval requirements for the production, distribution, and use of certain encryption technology was cause for optimism. In addition, the OSCCA's decision in May 2017 to authorize the Dutch semiconductor manufacturer NXP to develop and produce cryptography products in China—the first time that the OSCCA has granted a foreign company such a certification—also indicated that Chinese authorities might be inching toward liberalizing at least some facets of the country's encryption regime.

There is little reason to believe, however, that Beijing will abandon its concerns about national security or its desire for technological autonomy. In fact, Chinese policymakers are likely to see the trade war and the U.S. government's efforts to prevent the flow of technologies into China as a justification for redoubling attempts to reduce the country's dependence on foreign products. Indeed, even as China liberalizes certain aspects of the country's encryption regulatory regime, it might make other aspects more intensive. The latest draft of the MLPS 2.0 procurement framework, for instance, relaxes the domestic intellectual property requirement for level three and above, although it appears to increase scrutiny in other areas and expand the number of sectors that are classified at level three. In short, foreign influence on China's encryption debate has always been limited, and it will become even more so.

It is harder to predict how the interactions between Chinese users and the Chinese government will play out, especially as Beijing envisions its economy and methods of governance as increasingly dependent on big data and artificial intelligence. Even in its more limited form, focused on financial credit history, the social credit system will involve pooling large amounts of data, which could

exacerbate public concerns over personal data security. In a more extreme form, the social credit system could connect separate oceans of data to provide comprehensive scores of citizens' social, political, and financial reliability on a scope that is hard to comprehend. The government's big data surveillance already appears to have led to massive data leaks. If there are leaks or hacks of such data, and history suggests there will be, Chinese citizens will almost certainly demand greater protections, which could involve the wider use of encryption.

The Chinese government will continue to grapple with the tensions between satisfying public demands for responsibly handling and using citizens' data with the national security imperatives of achieving technological autonomy and leveraging technology to advance other governance objectives. The contours of this interplay will continue to have profound implications for the rest of the world.

About the Authors

Lorand Laskai is an incoming 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.

The authors would like to thank Paul Triolo for his expert review of the manuscript.

Notes

1 See, for example, the following documents: "Guojia Mima Guanliju guanyu fabu《Mima Shuyu》gonggao" [State Cryptography Administration public announcement regarding the release of its technical directive on cryptography standardization], State Cryptography Administration, Public Notice no. 25, June 20, 2013, http://www.oscca.gov.cn/sca/xwdt/2013-06/20/content_1002399.shtml; "Guojia Mima Guanliju guanyu fabu《IPSec VPN jishu guifan》deng 17 xiang mima hangye biaozhun gonggao" [State Cryptography Administration public announcement regarding the release of 17 cryptography industry standards for Internet Protocol Security and VPN technology], State Cryptography Administration, Public Notice no. 28, February 13, 2014, http://www.oscca.gov.cn/sca/xwdt/2014-02/13/content_1002404.shtml; and "Guojia Mima Guanliju guanyu fabu《Mima Mokuai Anquan Jiance Yaoqiu》deng 5 xiang mima hangye biaozhun gonggao" [State Cryptography Administration public announcement regarding the release of 5 industry standards on the safety testing requirements of cryptography modules], State Cryptography Administration, Public Notice no. 29, April 1, 2015, http://www.oscca.gov.cn/sca/xwdt/2015-04/01/content_1002406.shtml.

2 The author thanks Paul Triolo for this point.

3 WLAN stands for wireless local area network.

4 James McGregor, *No Ancient Wisdom, No Followers: The Challenges of Chinese Authoritarian Capitalism* (Westport, CT: Prospecta Press, 2012), 40.

5 Because iMessage stores messages on iCloud by default, it provides a technical workaround for authorities to access user data.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

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

CarnegieEndowment.org