DIVERSE CHALLENGES • EMERGING TECHNOLOGIES • CREATIVE SOLUTIONS • DIVERSE CHALLENGES • EMERGING TECHNOLOGIES • CREATIVE SOLUTIONS

China’s Internet of Things

John Chen, Emily Walz, Brian Lafferty, Joe McReynolds, Kieran Green,
Jonathan Ray, and James Mulvenon

Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission

October 2018

Disclaimer: This research report was prepared at the request of the U.S.-China Economic and Security Review Commission to support its deliberations. Posting of the report to the Commission's website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 113-291. However, it does not necessarily imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed in this commissioned research report.

About the SOSi Special Programs Division

This project was conducted within SOSi's Special Programs Division (SPD), the premier open source and cultural intelligence exploitation cell for the U.S. intelligence community. Staffed by an experienced team of cleared analysts with advanced language skills, SPD's mission is to provide cutting-edge, open source and cultural intelligence support to the collection, analytical, and operational activities of the U.S. intelligence community, with the goal of achieving national strategic objectives. SPD accomplishes its mission through the conduct of objective, independent, and relevant research and analysis, under strict quality guidelines.

Comments may be sent to the General Manager of the Special Programs Division, Dr. James Mulvenon.

Dr. James Mulvenon
General Manager
Special Programs Division
SOS International
2650 Park Tower Drive, Suite 300
Vienna, VA 22180
TEL: 571-421-8359
Email: James.Mulvenon@sosi.com

Table of Contents

Acronym List

Acronym	**Term**
2G	Second Generation
3G	Third Generation
3GPP	Third-Generation Partnership Project
3PLA	General Staff Department 3rd Department
4G	Fourth Generation
4PLA	General Staff Department 4th Department
5G	Fifth Generation
5G NR	Fifth Generation New Radio
5GAA	Fifth Generation Automobile Association
ACR	Automated Content Recognition
AFNOR	*Association Française de Normalisation*
AI	Artificial Intelligence
AIOTI	Alliance for the Internet of Things Innovation
ANSI	American National Standards Institute
APEC	Asia Pacific Economic Cooperation
API	Application Programming Interface
APT	Advanced Persistent Threat
AQSIQ	General Administration of Quality Supervision, Inspection and Quarantine
AVIC	Aviation Industry Corporation of China
AWS	Amazon Web Services
BRI	Belt and Road Initiative
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAC	Cyberspace Administration of China
CAGR	Compound Annual Growth Rate
CAICT	China Academy of Information and Communications Technology
CAIH	China Aerospace Investment Holdings Ltd.
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing Act
CAS	Chinese Academy of Sciences
CAS IIE	Chinese Academy of Sciences' Institute of Information Engineering
CASC	China Aerospace Science and Technology Corporation
CASIC	China Aerospace Science and Industry Corporation
CBPR	Cross-Border Privacy Rules
CCC	China Compulsory Certification
CCP	Chinese Communist Party
CDI	Content Digital Innovation Technology Co., Ltd

CEO	Chief Executive Office
CETC	China Electronics Technology Group Corporation
CFIUS	Committee on Foreign Investment in the United States
CIA	Confidentiality, Integrity, and Availability
CMI	Civil-Military Integration
CMS	China Merchants Securities
CNITSEC	China Information Technology Evaluation Center Security Testing Center
CNKI	China National Knowledge Infrastructure
CNNVD	China National Vulnerability Database
CNO	Computer Network Operations
COPPA	Children’s Online Privacy Protection Rule
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CSIC	China Shipbuilding Industry Corporation
DAS	Data Acquisition Systems
DDoS	Distributed Denial of Service
DO	Digital Object
DOA	Digital Object Architecture
DoD	Department of Defense
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECV	Environmental Characteristics Value
EEA	European Economic Area
EEPROM	Electrically Erasable Programmable Read-Only Memory
eMBB	Enhanced Mobile Broadband
ETIRI	Electronic Technology Information Research Institute
ETSI	European Telecommunications Standards Institute
EU	European Union
EULA	End User License Agreement
FCRA	Fair Credit Reporting Act
FDA	Food and Drug Administration
FIRRMA	Foreign Investment Risk Review Modernization Act
FTC	Federal Trade Commission
FTCA	Federal Trade Commission Act
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GPS	Global Positioning System
GSMA	Global System for Mobile Communications Association
GTI	Global TD-LTE Initiative

HIPAA	Health Insurance Portability and Accountability Act
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
ID	Identification/Identity/Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IoV	Internet of Vehicles
IP	Intellectual Property
IP	Internet Protocol
IPR	Intellectual Property Rights
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITR	International Telecommunication Regulations
ITU	International Telecommunications Union
LAN	Local Area Network
LLC	Limited Liability Corporation
LPWAN	Low-Power Wide Area Networks
LSO	Local Storage Objects
LTE	Long-Term Evolution
M2M	Machine-to-Machine
MAC	Media Access Control
MANET	Mobile Ad-Hoc Network
MEC	Mobile Edge Computing / Multi-Access Edge Computing
MEMS	Microelectromechanical Systems
MIIT	Ministry of Industry and Information Technology
MIMO	Multiple-Input Multiple-Output
MLPS	Multi-Level Protection Scheme
MOST	Ministry of Science and Technology
MPS	Ministry of Public Security
MSS	Ministry of State Security
N/A	Not Applicable
NB-IoT	Narrowband IoT
NDA	Non-Disclosure Agreement
NDRC	National Development and Reform Commission

NGMN	Next Generation Mobile Networks Alliance
NGO	Non-Governmental Organization
NIST	U.S. National Institute of Standards and Technology
NORINCO Group	China North Industries Group Corporation
NR	New Radio
NUPT	Nanjing University of Posts & Telecommunications
NWU	Northwest University
OBOR	One Belt One Road
OECD	Organisation for Economic Co-operation and Development
OS	Operating System
PLA	People’s Liberation Army
PLMN	Public Land Mobile Network
PRC	People’s Republic of China
QR	Quick Response
R&D	Research and Development
RAN	Radio Access Network
RD&A	Research, Development, and Acquisition
RFID	Radio-Frequency Identification
RI	Research Institute
RMB	*Renminbi*
S&T	Science and Technology
SAC	Standardization Administration of the People’s Republic of China
SAIC	State Administration for Industry and Commerce
SASTIND	State Administration for Science and Technology for National Defense
SDK	Software Development Kit
SEMB	State Encryption Management Bureau
SEP	Standard-Essential Patent
SIM	Subscriber Identity Module
SIMIT	Shanghai Institute of Microsystem and Information Technology
SKLOIS	State Key Laboratory of Information Security
SMS	Short Message Service
SPAPSF	Special Project Action Plan for Standards Formulation
SSB	State Secrecy Bureau
SSL	Secure Sockets Layer
TC	Technical Committees
TCP/IP	Transmission Control Protocol/Internet Protocol
TD-LTE	Time Division Long-Term Evolution
TD-SCDMA	Time Division Synchronous Code Division Multiple Access

TLS	Transport Layer Security
TRB	Technical Reconnaissance Bureau
TV	Television
UAV	Unmanned Aerial Vehicle
UN	United Nations
U.S.	United States
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus
USCBC	U.S.-China Business Council
USD	United States Dollar
USTR	United States Trade Representative
UUV	Unmanned Underwater Vehicle
V2X	Vehicle-to-Everything
W3C	World Wide Web Consortium
WAPI	WLAN Authentication and Privacy Infrastructure
WIC	World Internet Conference
WLAN	Wireless Local Area Network
WSC	World Standards Cooperation
WTO	World Trade Organization

Executive Summary

The Internet of Things (IoT)—the interconnection of physical and virtual things via information and communication technologies—is emerging as the next front in global network infrastructure, with potentially transformative benefits across a range of applications and services. Due to its potential adoption in essentially all economic sectors, analysts expect the IoT to expand exponentially over the next few years, ultimately involving billions of connected devices and dozens or more vertical markets around the world. However, pressing questions about the IoT's operation, safety, and security have yet to be answered. What international standards will guide the development of IoT technologies and supporting infrastructure like 5G networks? How secure is the IoT and what are the risks of its vulnerabilities? How will U.S. consumer data be used and protected here and abroad?

China features prominently in all of these issues, and its drive to become a leader in the IoT poses sobering challenges to U.S. economic and security interests. This report examines how China's development of the IoT—bolstered by the Chinese government's efforts to harness national resources for its promotion—has put China in a position to credibly compete against the United States and other leaders in the emerging IoT industry. China's pursuit of IoT dominance constitutes a significant challenge to U.S. economic and national security interests. Its robust participation in international standards committees has given Beijing greater opportunities to dictate the rules of the road. Its research into IoT security vulnerabilities and its growing civil-military cooperation raise concerns about gaining unauthorized access to IoT devices and sensitive data. Its authorized access to the IoT data of U.S. consumers will only grow as Chinese IoT companies leverage their advantages in production and cost to gain market share in the United States.

For now, China's large market size, production capacity, and government support offer some significant advantages, but China is still behind leading international levels in many IoT technologies. Therefore, U.S. companies and the U.S. government still have time to maintain a technological edge and influence future IoT development, standards, and roll-out. By comparison, the world is on the cusp of 5G with commercial rollouts beginning in 2018. The countries with the largest and most reliable 5G networks will have a head start in developing the technologies that 5G enables–first among them, the IoT. China has laid a solid groundwork for a comprehensive rollout, relying on a whole-of-country approach that has created an entire ecosystem for domestically manufactured 5G technologies and furthered their inclusion in international technical standards. With ten times the 5G sites per person as in the United States, China appears likely to lead early 5G deployment.[1]

Chinese dominance in the IoT will likely come at considerable cost to U.S. companies and consumers, hurting both U.S. economic and national security interests. China sees technology development as a decisive strategic resource and believes other countries' control of key technologies is a significant strategic liability. Its determination to lead in IoT development is grounded in these considerations, as well as a high sensitivity to the cost of ceding dominance in next-generation technologies to other powers. As such, China's IoT development strategy to date has been designed to narrowly serve Chinese interests. The Chinese government is unlikely to

[1] Dan Littmann, Phil Wilson, Craig Wigginton et al., "5G: The Chance to Lead for a Decade" (London: Deloitte, 2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf?mod=article_inline.

show much consideration for the protection of U.S. consumers, let alone U.S. companies competing in the IoT space.

China's Approach to IoT Development

As this report describes, China's commitment to becoming a leader in IoT development is predicated on the belief that its security requires it to become a technological power, particularly in emerging technologies that the country considers strategically vital. The potential effect of the IoT on the global economy led Chinese leaders to designate it as a priority area for development in 2009. China subsequently took steps to catalyze domestic IoT research and development (R&D) and infrastructure development through robust planning initiatives and extensive financial support. After years of this support, the Chinese IoT market has grown rapidly, passing 1 trillion RMB (approx. $154 billion) in value in 2017, with expectations that it will reach 1.8 trillion RMB (approx. $264 billion) in value by 2020. Global IoT industry growth trends have been similarly robust: by way of comparison, some experts believe that IoT infrastructure investment is expected to reach $421 billion in the United States and $274 billion in Europe by 2021.[2] Chinese experts anticipate that an "Internet of Everything" era will arrive once IoT is adopted widely in developed countries, and some assess that China has already developed a relatively complete IoT supply chain, including chips, components, devices, software, systems integration, operators, and applied services.

China's top leaders have long viewed technological advancement as a bellwether of national strength and security and are keen to avoid falling behind other international competitors in technological advancement. Driven by this sense of urgency, China's policies to promote IoT development have included the creation of IoT industrial clusters and demonstration bases, extensive financial support for IoT R&D, restrictions on foreign investment, selective enforcement of Chinese laws to hinder the operation of foreign IoT firms in China, and the ever-looming prospect of technology transfer.

These policies pose serious challenges for U.S. firms competing with Chinese firms in the IoT industry, who must be aware that the Chinese government considers them to be strategic rivals, if not outright threats. China is likely to engage in protectionist and unfair trade practices to favor its own IoT companies over foreign competitors, creating an austere and tacitly hostile market environment for foreign firms. In response, this report recommends that the U.S. government:

- Commission a blue-ribbon panel with a mandate to assess the ability of the United States to compete in emerging commercial information and communications technologies;
- Publish a list of federal guidelines laying out "best practices" for IoT firms seeking to operate within China;
- Continue to seek legal redress against coercive Chinese trade practices through international institutions; and
- Collaborate with partner nations to counter coercive Chinese trade practices and expand existing trade partnerships in the Asia-Pacific region to build a larger shared market that could act as a counterweight to China's economic power.

[2] "Worldwide Semiannual Internet of Things Spending Guide," IDC, accessed September 5, 2018, https://www.idc.com/getdoc.jsp?containerId=IDC_P29475

China's Race to Set International Technical Standards

The Chinese government is actively attempting to influence international technical standards for the IoT that would benefit Chinese companies at the expense of U.S. and other foreign counterparts. As information technology (IT) industry precedents have shown, the competition over technical standards touches on a larger contest about intellectual property ownership, market advantage, international prestige, and approaches to privacy, security, and control of data. Once a global standard is established and accepted it can put pressure on countries or companies developing other standards to conform to the existing norm, ceding these important benefits to whichever nation's preferences manage to be adopted as the international standard. This advantage is magnified from a security viewpoint, as the originator of a standard technology has an intimate understanding of how it operates inside and out. China's increased effort to influence and set international IoT standards is a critical part of China's ambitious state-directed plan to achieve dominance in the IoT. These efforts may lock-in Chinese preferences for standards in IoT and supporting infrastructure sooner rather than later, as nascent IoT and 5G standards exist in a fragmented and complex standards-setting environment rife with incompatible proprietary solutions and an alphabet soup of standards-setting bodies.

China is currently leveraging a more coordinated and comprehensive strategy than the United States to influence relevant standards for the IoT, and U.S. entities are often absent from key international standardization processes. Consequently, some international standards have been developed with reduced U.S. input. In contrast, China's international standardization efforts are increasing, following a centralized plan to effect change at both high and ground levels. On the high level, China has increased its participation in international standards institutions, where it shows a preference for multilateral (one country, one vote) standards institutions over U.S.-backed multi-stakeholder institutions. Chinese nominees leading these organizations work in tandem with national Chinese standards development efforts and push China's agenda from their official platforms. On the ground level, China is leveraging the country's sizable economy, state investment in new technologies, and state-subsidized foreign policy initiatives like the Belt and Road Initiative (BRI) to encourage other countries to adopt its technology, and with it, its standards. China is explicit in its support for "standardization work" and will likely continue emphasizing this work and strategy for the IoT and other new and emerging technologies.

To address China's aggressive pursuit of international technical standards and ensure U.S. leadership and advantages in the IoT and other related industries, the U.S. government should:

- Conduct additional open source reporting and research on China's international standards efforts;
- Encourage more U.S. participation in international standards committees through additional funding and incentives;
- Where acceptable, adopt proposals and processes agreed upon by multi-stakeholder international standardization bodies while continuing to counter Chinese attempts to re-define internet governance as a matter of national sovereignty that requires the devolution of control to nation-states; and
- Create a government-industry advisory body charged with studying corporate foreign interactions in the interest of national security.

Unauthorized Access to IoT Devices and Chinese Exploitation Efforts

The IoT is inherently vulnerable to attack as billions of devices are added and connected to networks. These products, from industrial controls to smart watches, can become attack surfaces through their internet connections. Worse, market demands for lower costs paired with low barriers to entry in the IoT market mean there is currently little incentive to build more secure IoT devices. Unauthorized access to IoT devices has already resulted in physical consequences, including attacks on industrial machinery and power grids around the world. Future unauthorized access is likely to open a Pandora's box of negative consequences as IoT devices are deployed in greater numbers around the world.

Because of its market size, China has the potential to wield an outsize impact on the security of IoT devices against unauthorized access (i.e., technical compromise). Chinese-manufactured IoT devices have already become common targets for unauthorized access, thanks in part to insecure device configurations that have resulted in surreptitious data collection and the commandeering of devices for use in botnets. The widespread usage of Chinese IoT devices and components suggests that the aggregate negative consequences of unauthorized access to Chinese devices may be proportionally larger than for devices from other countries.

China is also actively researching IoT vulnerabilities, both for security purposes and almost certainly to collect intelligence, conduct network reconnaissance for cyberattacks, and enhance its domestic surveillance powers. Chinese IoT security research exhibits a familiarity with exploitation methods that could lead to unauthorized access and is already leveraging machine learning and algorithmic techniques to accelerate the pace of research and develop adaptable malicious code that could affect multiple types of IoT devices. China's IoT security research entities are also part of a broader and increasingly fused civil-military research ecosystem that increases the chances that PRC intelligence and military actors will have access to any breakthroughs in IoT vulnerability research.

The combination of widespread adoption of IoT products and Chinese research into exploits raises the threat of unauthorized access to U.S.-based IoT devices and the networks they connect to. To counter Chinese potential exploits of IoT vulnerabilities and safeguard U.S.-based devices against state and non-state threats, the U.S. government should:

- Encourage adoption of security best practices for IoT products in the form of an industry-backed cybersecurity program;
- Increase funding and support for IoT security research, especially in areas that could yield proportionately greater gains for IoT security;
- Document Chinese entities that conduct IoT security research for, alongside, and supported by Chinese military and security services; and
- Overhaul the oversight process for green-lighting Chinese investment in U.S. IoT industry in order to better account for the unique security concerns posed by China's blending of its military and civilian IoT research ecosystems.

Authorized Access to IoT Data and Privacy Concerns

While authorized data access, collection, and processing are indispensable parts of the IoT's transformative potential, the Chinese government is uniquely empowered to access the IoT data of U.S.-based consumers. Authorized access, or access that is agreed to by the consumer in lengthy terms and conditions documents, allows companies and governments to gather massive amounts of data that can translate into substantial economic and strategic advantages. While this practice is the norm across the world, China poses a grave threat to U.S. privacy as its government and surveillance apparatuses are empowered to access this data well in excess of accepted international norms. Chinese companies can access U.S. IoT data in four main ways:

1. At the user-level, Chinese entities can access U.S. data simply from sales and usage of their IoT products by U.S. consumers who authorized data collection and transmission by agreeing to terms of use.
2. Device-level access through the device manufacturing and design process opens up opportunities for outside entities to collect even more information at scale.
3. At the corporate level, Chinese companies could buy U.S. IoT companies and the data they have accumulated through their products, or buy U.S. data through a third-party vendor or a data broker.
4. Last, Chinese government data appropriation powers could expose U.S. IoT data to Chinese government collection.

Chinese access to U.S. IoT data is problematic for U.S. national security and economic competitiveness. In the short term, Chinese government and corporate access to U.S. data would be a huge opportunity for Chinese intelligence targeting operations. In the longer term, such access would provide a major edge to Chinese artificial intelligence (AI) development efforts, eventually culminating in a substantial Chinese economic advantage in another field that is expected to shape the economy of the future.

Existing U.S. data protections appear insufficient to protect U.S. data against harmful but authorized data access. The patchwork nature of U.S. laws and authorities leaves loopholes that could facilitate Chinese access to U.S. IoT data in bulk, an especially risky proposition given known Chinese motivations for accessing big data. To address these deficits, the U.S. government should:

- Enact a tiered disclosure regime for IoT products broad enough to cover multiple aspects of authorized IoT data collection;
- Mandate data expiration and de-identification of data where appropriate according to existing principles of data minimization, especially for information resellers;
- Codify existing U.S. data regulations and others in a single, comprehensive federal law governing data privacy;
- Require foreign IoT products to disclose affiliation with foreign entities that may pose a significant risk of harmful but authorized access to U.S. data;
- Refer corporate-level attempts to transfer U.S. data to foreign entities to CFIUS for approval; and
- Expedite passage of a unified federal data privacy statute applicable to both foreign and domestic IoT companies.

Conclusions

The United States can counter or blunt the challenge from China in many areas through sound policy. A comprehensive accounting of Chinese participation in key international standards bodies would identify areas that might require more U.S. involvement. More exhaustive studies of the effectiveness of European data privacy protections may help determine what model of data protection would be most effective in closing the front door to the IoT data of U.S. citizens. Some of these countermeasures require only U.S. action and do not depend upon Chinese cooperation.

In other areas of IoT development, however, the U.S. ability to protect its own interests and those of its citizens will be limited. For example, the one-party Chinese regime is simply more empowered to demand all data collected by Chinese IoT companies, including data from U.S. consumers. Although the U.S. government could theoretically prevent U.S. companies from turning over the data they hold to Chinese entities, there is little it can do to prevent the Chinese government from obtaining such information once it is in the hands of Chinese companies. This reality demands a clear-eyed understanding of these challenges and needs greater coordination between the resources of Washington, the innovative capacity of the U.S. private sector, and perhaps coordinated efforts with U.S. allies abroad. Participation in international standards bodies, long overdue data privacy legislation, and industry best practices for IoT security would benefit from such coordination and help mitigate the challenges from Beijing.

Introduction and Methodology

The “Internet of Things” (IoT) refers to the network of physical devices and items with embedded sensors and network connections that allow them to connect to each other and to the broader internet. The IoT, along with critical supporting infrastructure such as artificial intelligence, cloud computing, and fifth generation (5G) wireless technology, is beginning to evolve into mature technological ecosystems, attracting considerable attention from governments, companies, and the public along the way.

The IoT and 5G are topics *du jour* for good reason. The IoT fundamentally represents a nearly unlimited opportunity to optimize every aspect of our physical lives through data, while 5G wireless technology enables the deployment of the IoT to previously untouched areas using previously unattainable connection speeds. On the one hand, the proliferation of IoT devices, the data they produce, and the wireless infrastructure they rely upon are projected to generate potentially trillions of dollars in revenue and bring dramatic and unprecedented change to the lives of many. On the other hand, the breakneck pace of IoT development threatens to outrun the security and privacy regulations needed to ensure safe and appropriate use of the IoT. Security vulnerabilities inherent in IoT devices and the lack of regulation for the data they produce are likely to threaten both IoT users and the entire internet ecosystem within which the IoT resides.

China’s leaders began to embrace the groundbreaking implications of the IoT at a high level as early as 2009, when the IoT was identified as one of five “strategic emerging industries” (新兴战略产业) by then-Premier Wen Jiabao.[3] Hu Jintao, then-Chinese Communist Party (CCP) Chairman, lent his imprimatur to the effort shortly thereafter in a 2010 speech,[4] and by 2012, these high-level endorsements had been translated into a wide-ranging, state-run approach to IoT development characterized by the issuance of a variety of state plans in different IoT-related fields. China’s IoT development has progressed by leaps and bounds under government tutelage and with substantial government monetary and policy support.

China’s state-led approach to IoT development has shaped Chinese technological policymaking, with significant consequences for U.S. economic and national security interests. Chinese IoT experts are actively engaged in efforts to influence international IoT and 5G standards that may one day “lock in” Chinese advantages in production and cost while positioning Beijing to dominate the IoT sector writ large. Chinese military and civilian researchers are energetically studying IoT security vulnerabilities that could one day be built in to trillions of IoT devices manufactured to comply with China’s preferred international standards. Recent Chinese legislation explicitly enables the regime to commandeer any data deemed necessary to protect national security, while Chinese companies subject to these laws rush to acquire as much IoT data as possible. Many of

[3] Ministry of Science and Technology of the People’s Republic of China, “中国科学技术发展报告 2009” (China Science and Technology Development Report 2009), March 3, 2010, http://www.most.gov.cn/kjfz/kjxz/2009/201103/P020110307528692348585.pdf.

[4] Hu Jintao 胡锦涛, “胡锦涛在 2010 年两院院士大会上的讲话” [Hu Jintao’s Speech at the Personnel Conference of the Two Academies], June 7, 2010, http://scitech.people.com.cn/GB/11810084.html.

these efforts are guided by Chinese Paramount Leader (最高领导人)[5] Xi Jinping's dictum that "there can be no national security without network security."[6]

This report documents various aspects of China's state-led approach to IoT development, discusses their economic and national security implications for the United States, and makes recommendations for U.S. decision-makers to address these implications where possible. Chapter 1 provides an overview of China's IoT development, describing a concerted, state-led effort to become the premier nation in IoT innovation and assessing successes and challenges in China's IoT development to date. Chapter 2 details ongoing Chinese efforts to influence international IoT standards as a critical component of China's overall effort to dominate the IoT sector. Chapter 3 discusses Chinese military and civilian research into IoT security vulnerabilities, illustrating the risks of unauthorized access, use, and exploitation of IoT devices by the Chinese state and third parties should China ever achieve dominance in the IoT sector. Finally, Chapter 4 assesses how the IoT may enable Chinese access to the information of U.S. citizens through a combination of authorized disclosure and sweeping Chinese government data access powers. The report concludes with a summary of the findings from the chapters and a brief assessment of areas that may require further study.

Each chapter of this report is based on open source research and uses commonly cited concepts to characterize China's approach to IoT development. Information in this report was sourced from academic publications, corporate websites, news media, and other online content, with a special emphasis on Chinese-language sources. Specifically, Chapters 1 and 2 describe Chinese intentions for IoT development through a close reading of official Chinese state planning documents in the original Chinese and document the implementation of these efforts through extensive use of available media reports. Chapters 3 and 4 examine the security and privacy of the IoT by assessing Chinese access to IoT devices and data based on the commonly cited information security concept of authorization, defined as access privileges granted to a user, program, or process.

The sheer scale and pace of China's IoT development efforts make an exhaustive accounting of Chinese efforts impossible within the scope of this report. A full-scale, quantitative documentation of Chinese state planning, international standardization efforts, IoT vulnerability research, and IoT device license agreements would be immensely helpful but falls well outside the parameters of this report. Instead, this report highlights useful information for U.S. stakeholders by detailing the broader trends, contours, and implications of Chinese IoT development using appropriately illustrative examples.

[5] The title "paramount leader" is an informal term used to refer to the most prominent political leader in the People's Republic of China, who generally is head of state, head of the Chinese Communist Party, and head of the military.

[6] Yang Ting 杨婷, ed., "习近平: 把我国从网络大国建设成为网络强国" (Xi Jinping: Transform China from an Internet Great Power to a Strong Internet Power), Xinhua, February 27, 2014, http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

Chapter 1: Overview of China’s IoT Development

China’s approach to Internet of Things (IoT) development is fundamentally characterized by the promulgation of multiple overlapping government directives and justified by mandates from China’s top leaders and central economic planners. While academic institutions and private companies are undoubtedly important drivers of innovation and market capture, the Chinese IoT sector benefits considerably from government policy coordination and financial support that reflects Beijing’s high prioritization of IoT development. Specially arranged government funds dispense money for R&D, while various state-issued mandates direct government ministries to coordinate policies in pursuit of faster and more widespread adoption of the IoT.

Much of the impetus for this government-accelerated IoT development stems from China’s techno-nationalist view of IT advancements.[7] China’s top leaders have long viewed technological advancement as a bellwether of national strength and security and are keen to avoid falling behind other international competitors in technological advancement. The IoT is viewed as an especially important type of IT with the potential to have a considerable transformative impact on China’s economy and national strength.

Despite this considerable government support, Chinese officials continue to perceive several weaknesses in Chinese IoT development. Issues such as a decentralized supply chain, divergent standards, and limited adoption of IoT devices in various industries appear to hinder China’s overall drive for IoT dominance.

Regardless of the actual strengths or weaknesses of China’s IoT development, the country’s top-down, government-supported approach has undeniable consequences for U.S. IoT firms. The strategic importance that Beijing places on Chinese IoT development likely means that many of these consequences are negative. U.S. IoT firms seeking entry into China’s vast IoT market face restrictions on foreign investment, selective enforcement of Chinese laws, and the prospect of involuntary or detrimental technology transfer. Ultimately, China’s strategic emphasis on IoT development is underpinned by a competitive drive that may place U.S. national security and economic interests in jeopardy.

[7] For more on the history and implications of China’s techno-nationalism, see Jonathan Ray, “Red China’s ‘Capitalist Bomb’: Inside the Chinese Neutron Bomb Program,” *China Strategic Perspectives* 8, (Washington, DC: National Defense University Press, 2015); and Evan A. Feigenbaum, *China’s Techno-Warriors: National Security and Strategic Competition from the Nuclear to the Information Age* (Stanford: Stanford University Press, 2003).

China's IoT Development Strategy

While China's strategy for IoT development is not found in a single unified document, the contours of Beijing's strategy are clearly drawn by China's highest officials, economic planners, and technical experts. The following sections describe working definitions of the IoT ecosystem, Chinese justification for accelerated IoT development, and the broader techno-nationalist context of China's IoT strategy.

Defining and Describing the IoT Ecosystem

The IoT defies concise definition thanks to its broad potential application and continuing evolution and development. While some authoritative organizations like the International Telecommunications Union (ITU) have attempted to broadly describe the IoT and its constituent elements,[8] the U.S. National Institute of Standards and Technology (NIST) has so far deliberately avoided defining the IoT in its authoritative glossary of information technology terms.[9] Despite this lack of consensus on a precise definition, a number of characterizations of the IoT have emerged. One recent Cisco textbook describes the IoT as a "combination of endpoints or things, connectivity, and people and processes, with interactions (data and decisions) between these entities creating smart systems and services that deliver business value." [10] International standardization bodies like the ITU view the IoT as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)."[11]

One reason why the IoT continues to defy simple definition is that the basic underlying technologies of the IoT are widely applied in multiple industries in different forms. For instance, the sensors in a network-connected pacemaker are many times smaller and respond to different stimuli than those in a smart car, but both carry out the same basic function of measuring physical properties. It is therefore frequently difficult to envision exactly what a future IoT sensor may look like, and the many possible IoT applications may complicate efforts to scale up IoT development.

Given the wide variety of possible applications of the IoT, some organizations have avoided definitions in favor of descriptions of its main components and functionality. A 2016 report from NIST notes that at its core, the IoT "involves sensing, computing, communication, and actuation."[12] To these ends, NIST identifies the main building blocks of any network of things (including IoT) as sensors, aggregators, communication channels, external utilities, and decision triggers. These components, their definitions, and their functions are described briefly in the table below.

[8] "Overview of the Internet of Things, Recommendation ITU-T Y.2060," United Nations International Telecommunications Union, July 15, 2012, http://handle.itu.int/11.1002/1000/11559-en?locatt=format:pdf&auth.

[9] United States Department of Commerce, National Institute of Standards and Technology, "Glossary," *NIST Computer Security Resource Center,* accessed July 7, 2018, https://csrc.nist.gov/Glossary/?term=6476#AlphaIndexDiv.

[10] Anthony Sabella, Rik Irons-Mclean, and Marcelo Yannuzzi, *Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT* (Indianapolis, IN: Cisco Press, 2018), Chapter 1.

[11] "Overview of the Internet of Things, Recommendation ITU-T Y.2060," United Nations International Telecommunications Union.

[12] Jeffrey Voas, "Networks of 'Things,'" NIST Special Publication 800-183, July 2016, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf.

Table 1: Building Blocks of the IoT[13]

Components	Function	Definition
Sensor	Sensing	Electronic utility that measures physical properties
Aggregator	Computing	Software that transforms raw data into aggregated data
Communication Channel	Communication	Medium by which data is transmitted
External Utility	Computing	Software or hardware product or service that execute processes or feed data into a network of things
Decision Trigger	Actuation	Creates the final results needed to satisfy purpose, specification, and requirements of a network of things

Analysts argue that the IoT industry is likely to benefit significantly from the continued advancement and maturation of other related technologies like cloud computing, fifth generation (5G) wireless technology, and low-power wide area networks (LPWAN). Cloud computing and related technologies (such as fog and edge computing[14]) will enhance the performance of sensors, aggregators, and external utilities deployed in various parts of an IoT network by making more capable computing resources available to IoT devices and sensors with limited onboard computing capacity.[15] 5G wireless technology is expected to enhance the communication functionality of the IoT by providing faster connectivity speeds and a more adaptive network reconfiguration to handle the huge amounts of traffic the IoT will generate.[16] This new generation of wireless technology offers data speeds up to fifty or a hundred times faster than current 4G networks by utilizing denser arrays of small antennas and the cloud.[17] This will enable billions of IoT devices to communicate with each other more efficiently, providing critical infrastructure backbone for industries and emerging technologies like self-driving cars and immersive networking. For their part, LPWANs are a method of connectivity characterized by long-distance transmission, low data rate, and low power consumption capabilities.[18] LPWAN technologies are still in their development phase, but are considered ideally suited for many IoT applications, and an upgrade over current technologies

[13] This table is derived from information in Jeffrey Voas, "Networks of 'Things.'" The publication refers to "Networks of Things" while considering the Internet of Things as a special type of a Network of Things.

[14] 'Edge computing' refers to the deployment of cloud computing resources in close proximity to where the data is produced. 'Fog computing' is sometimes used interchangeably with edge computing, but it is also used as a superset of edge computing, and connotes a broader continuum of space between the edge and the cloud. "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are," CISCO Systems Inc. White Paper, April 2015, https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf; "What's the Difference between MEC and Fog Computing?" SDxCentral, LLC, accessed September 4, 2018, https://www.sdxcentral.com/mec/definitions/whats-difference-mec-fog-computing/.

[15] David Hanes, Gonzalo Salgueiro, and Rob Barton, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things* (Indianapolis, IN: Cisco Press, 2017), Chapter 2.

[16] William Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (Addison-Wesley Professional, 2015), Chapter 1, Section 5.

[17] Rod Tucker, "5G vs NBN: Next-Gen Mobile Network will be a Convenient but Expensive Alternative," Australian Broadcasting Corporation, October 26, 2017, http://www.abc.net.au/news/2017-10-25/5g-vs-nbn-mobile-network-convenient-but-expensive-alternative/9083746.

[18] Rashmi Sharan Sinha, Yiqiao Wei, and Seung-Hoon Hwang, "A Survey on LPWA Technology: LoRa and NB-Iot," ICT Express, No. 1 (2017): 14-21.

like short-range radio technologies (e.g., Bluetooth), which cannot transmit data over long distances, and cellular technologies (e.g., 3G, 4G, 4G LTE), which have much higher power consumption.[19]

Artificial intelligence (AI), another related technology, is likely to both enhance IoT development and benefit greatly from more widespread IoT adoption. Improvements in AI could improve decision triggers for IoT systems by making sense of large amounts of data and managing the IoT system accordingly to achieve optimal results.[20] One IoT expert at IBM declared that AI's role is to be "the brain running IoT systems."[21] Widespread IoT adoption could also greatly enhance AI development. Combining the data derived from IoT-enabled devices with AI means smart devices will increasingly integrate AI algorithms, which can support optimizing and adapting IoT devices and infrastructure.[22] Applied on a wide enough scale, analysts expect that AI will enable an "Internet of Everything" (IoE)—characterized by devices sharing data between people, between machines, and between people and machines across all network-connected systems—that supplants the IoT.[23]

China's state-led IoT development efforts are part of a broader national effort to accelerate China's development and superiority in several critical technology areas, with a special focus on AI. Government plans to develop AI strongly emphasize IoT development, explicitly linking the role of the IoT to the value of data collection for future AI applications, and also stress the increased deployment of 5G infrastructure to support AI. The 2017 "New Generation Artificial Intelligence Development Plan" (新一代人工智能发展规划) mandates developing "high-sensitivity and highly reliable smart sensors and chips that support the new-generation Internet of Things," and prioritizes progress in "core Internet of Things technologies such as RFID and short-distance machine-to-machine communication, as well as key components like low-power processors."[24] The plan also calls for China to perfect IoT infrastructure and coordinate the use of big data infrastructure to provide extensive support for AI research and development (R&D) and broader applications, as IoT is expected to play a critical role in smart manufacturing, smart industrial support, and smart driving networks.[25] Overall, China's approach acknowledges the tightly interwoven relationships between the IoT, its basic constituent components, and technology areas

[19] Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer, "A Comparative Study of LPWAN Technologies for Large-Scale IoT Deployment," ICT Express, January 4, 2018, https://reader.elsevier.com/reader/sd/E34473F242F28C96E6C761117DB55136EC2935DA7AC601FA0774F8F2F0E59D945C6F90D90A67F2173283B1EE62A3C98A.

[20] David Hanes, Gonzalo Salgueiro, and Rob Barton, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things* (Indianapolis, IN: Cisco Press, 2017), Chapter 1.

[21] Bernard Marr, "The Internet of Things (IoT) Will Be Massive in 2018," *Forbes,* January 4, 2018, https://www.forbes.com/sites/bernardmarr/2018/01/04/the-internet-of-things-iot-will-be-massive-in-2018-here-are-the-4-predictions-from-ibm/#54c92a43edd3.

[22] Ahmed Banafa, "Eight Trends of the Internet of Things in 2018," *IEEE,* January 9, 2018, https://iot.ieee.org/home/sitemap/46-newsletter/january-2018.html.

[23] Tom Snyder and Greg Byrd, "The Internet of Everything," *Computer*, June 2017, https://www.computer.org/csdl/mags/co/2017/06/mco2017060008.pdf.

[24] "新一代人工智能发展规划" (New Generation Artificial Intelligence Development Plan), State Council of the People's Republic of China, July 8, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

[25] "新一代人工智能发展规划" (New Generation Artificial Intelligence Development Plan), State Council of the People's Republic of China, July 8, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

like 5G, AI, and cloud computing as critical parts of its national economic development and security.

In China, the government's understanding of the IoT has been significantly guided by the foundational policy research carried out by the Ministry of Industry and Information Technology (MIIT) via its subordinate China Academy of Telecommunication Research.[26] The latter's "2011 IoT White Paper" defined IoT as:

> An expanded application of communication networks and the internet, which uses sensor technology and smart devices to perceive and recognize the physical world, and network connections to carry out calculations, processing, and data mining, in order to achieve information exchange and seamless connections between people and objects, or objects and objects. It reaches the goal of providing real-time control, precision management, and scientific decision-making vis-à-vis the physical world.[27]

The 2011 IoT White Paper conceptualized the IoT network framework as comprising three layers: a sensor layer made up of sensors, actuators, radio-frequency identification (RFID),[28] Quick Response (QR) codes, and smart devices; a network layer made up of IoT gateways that provide an IP address and connect to networks; and an application layer made up of application middleware and infrastructure that enables the use of the IoT in various areas. Given the breadth of this framework, the White Paper acknowledged that "an extremely high" number of key technologies are involved in the Internet of Things.[29] These included: high and low frequency RFID, smart sensors, location-aware sensors, MEMS sensors, short-range wireless communication technology and sensor nodes, mass information storage and processing, data mining, smart video image analysis, chips, sensor miniaturization, real-time location services, and information security, among others.

The IoT is filling a variety of roles across an ever-growing spectrum of applications. The latter ranges from early IoT application areas like utilities, where it enables remote meter reading and power transmission monitoring, and logistics, which uses IoT for smart inventory management, product transport, and warehouse monitoring; to more recent application areas like vehicles, where the IoT enables driverless car technology; and wearable devices, where the IoT is used for smart

[26] Li Renbo 李仁波, "业绩稳定增长，物联网发展迎来黄金时期" (With Stable Growth in Performance, Internet of Things Development Has Ushered in a Golden Age), 联讯证券 *Lianxun Securities*, May 8, 2018, 15. The China Academy of Telecommunication Research (电信研究院) is currently known as the China Academy of Information and Communications Technology (CAICT / 中国信息通信研究院), after a name change in 2014. "我院简介," China Academy of Information and Communications Technology, accessed July 17, 2018, www2.caict.ac.cn/wygk/.

[27] "物联网白皮书 (2011 年)" [2011 White Paper on IoT], China Academy of Telecommunication Research of MIIT 工业和信息化部电信研究院, May 2011: 15-16, www.miit.gov.cn/newweb/n1146312/n1146909/n1146991/n1648536/c3489477/part/3489478.pdf.

[28] According to the *RFID Journal*, RFID is "a generic term for technologies that use radio waves to automatically identify people or objects. There are several methods of identification, but the most common is to store a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification information to a reader. The reader converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it." "Frequently Asked Questions," RFID Journal, accessed September 4, 2018, https://www.rfidjournal.com/faq/show?49.

[29] [2011 White Paper on IoT], China Academy of Telecommunication Research of MIIT.

watches and personal activity trackers. In industry jargon, these application areas are known as verticals, since they are each capable of sustaining their own (vertical) industry ecosystem of devices, software, and product supply chains.

Competing for Primacy: Chinese Views on IoT Development

With respect to IoT policymaking, Chinese officials have portrayed their approach as part of a new era of Chinese technology policy that incorporates major lessons from the challenges encountered in the development of China's information technology (IT) industry in the 1990s and early 2000s. In an August 2009 inspection of the Chinese Academy of Sciences' Wuxi R&D Center for Micro-Nano Sensor Network Project Technology (中科院无锡微纳传感网工程技术研发中心), then-Premier Wen Jiabao decried the disadvantages China had faced from not being leading innovators in information technology, stating, "When the computer and internet industries were developing at a large scale, we went down some wrong paths because we did not master core technologies."[30] Wen directly linked these prior missed opportunities to China's plans for developing emerging IoT technologies, announcing that for IoT development China needed to "plan for the future a little earlier, and make core technology breakthroughs a little sooner."[31]

In 1999, the Chinese Academy of Sciences Shanghai Institute of Microsystem and Information Technology (SIMIT) and several universities initiated Chinese research into IoT, and the government provided "several hundred million RMB" for early technological and standardization research.[32] However, Chinese sources uniformly cite Wen's 2009 remarks as the event signaling the government's official support for IoT, after which it was named as a "strategic emerging industry" (新兴战略性产业) prioritized for development.[33] In his 2010 government work report, Premier Wen outlined the stakes for IoT, stating,

[30] Feng Songlin 封松林, "物联网的故事——写在"科学的春天"40 年之际" (Story of Internet of Things–Draft at 40th Anniversary of 'Springtime of Science'), *Bulletin of Chinese Academy of Sciences* 中国科学院院刊, no. 4, (2018): 439-441, accessed May 16, 2018, http://www.bulletin.cas.cn/publish_article/2018/4/20180419.htm.

[31] Feng, "Story of Internet of Things," 439-441.

[32] Wu Chengzhi 吴承治, "物联网——打造未来经济的引擎" (Internet of Things–Building the Engine of the Future Economy), 现代传输 *Modern Transmission*, no. 6 (2009): 14-19; "上海推进物联网产业发展行动方案 (2010–2012)" (Shanghai Action Plan for Promoting the Development of the IoT Industry (2010–2012)), Shanghai Municipal Commission of Economy and Informatization, accessed July 17, 2018, www.sheitc.gov.cn/res_base/sheitc_gov_cn_www/upload/article/file/2011_2/5_31/wscngoc6j6pu.doc. The imprecision of the investment figures cited by the author ("several hundred million RMB" over a period of ten years) makes it impossible to estimate an accurate dollar equivalent to this investment. However, the minimum figure–using the January 1, 2009 RMB to U.S. dollar exchange rate and 200 million RMB as the minimum stand-in for "several hundred million RMB"–was roughly $29 million. "Current and Historical Rate Tables," xe.com, January 1, 2009, accessed July 12, 2018, www.xe.com/currencytables/?from=CNY&date=2009-01-01.

[33] "我国物联网中心有望落户上海" [China's Internet of Things Center Will Hopefully Settle in Shanghai], *People's Daily Online 人民网*, February 23, 2010, http://society.people.com.cn/GB/97734/11010677.html.

> The global financial crisis is hastening the birth of a new technological and industrial revolution. It is of decisive importance for the future of our country that we develop emerging industries of strategic importance and capture the economic, scientific and technological high ground; therefore, we must seize opportunities, identify priorities, and achieve results…. We will… accelerate R&D in and application of the Internet of Things.[34]

The government's high prioritization of the IoT reflected the assessment of Chinese IT industry experts, who touted its "immense" (巨大) market potential as the next critical technology for the communication industry.[35] Chinese officials like MIIT Minister Miao Wei, MIIT Deputy Minister Xi Guohua, and head of the MIIT Science and Technology Department Wen Ku used public forums to highlight the IoT's economic importance as well, making their case in explicitly economic terms.[36] As Minister Miao stated in a 2011 article,

> IoT offers significant growth potential. It is a strong driving force [for economic growth], and it offers comprehensive positive benefits. It not only contains huge strategic growth potential, but can also effectively promote the deep integration of informationization and industrialization, drive the transformation and upgrading of traditional industries, and promote new economic growth points.[37]

China's promotion of IoT development was intensified by fears of missed opportunities. As MIIT's "12th Five Year Plan Development Plan for the Internet of Things" (物联网'十二五'发展规划), released in February 2012, observed,

[34] Wen Jiabao, "Report on the Work of the Government (2010)," The Central People's Government of the People's Republic of China, accessed May 17, 2018, http://www.gov.cn/english/official/2010-03/15/content_1556124_8.htm.

[35] Wang Weihong 王卫宏, "物联网的发展与相关产业价值链" (Evolution of the Internet of Things and the Related Value Chain), *Telecom Engineering Technics and Standardization* 电信工程技术与标准化, no. 12, (2009): 10-11; Wu Chengzhi 吴承治, (Internet of Things–Building the Engine of the Future Economy), *Modern Transmission*; Zhang Nan 张南, "'感知中国'高峰论坛召开中国移动：物联网是'万亿级'产业" ('Sensing China' Summit Forum Convenes–China Mobile: Internet of Things is a 'Trillion RMB' Industry), 通信世界 *Communications World*, no. 36 (2009): A7.

[36] "奚国华:物联网市场潜力巨大" [Xi Guohua: The Internet of Things' Market Potential is Immense], Phoenix Network 凤凰网, December 24, 2010, http://finance.ifeng.com/stock/special/wlbk/20101224/3108586.shtml; "工信部: 中国物联网万亿级市场规模须 10 年后" [MIIT: China's Trillion RMB IoT Market Will Not Arrive for at Least Ten Years], OFweek, November 8, 2010, http://iot.ofweek.com/2010-11/ART-132211-8110-28752734.html; Miao Wei 苗圩, "推进物联网产业快速有序发展" (Advance the Quick and Orderly Development of the IoT Industry), *Seeking Truth* 求是, no. 16 (2011), August 15, 2011, http://www.qstheory.cn/zxdk/2011/201116/201108/t20110815_102155.htm.

[37] Miao Wei 苗圩, (Advance the Quick and Orderly Development of the IoT Industry).

> International competition in IoT is becoming increasingly fierce: the United States has upgraded the Internet of Things to one of the most important priorities of its national innovation strategy; the European Union has developed a 14 points action plan to promote the development of the Internet of Things; Internet of Things is regarded as one of the four strategic priority areas of the U-Japan program; and South Korea's IT839 strategy identifies IoT as one of its three priority infrastructure construction programs.[38]

From China's perspective, one of the more problematic aspects of these programs in the United States, the European Union, and elsewhere was that they had launched before the Chinese government had its own IoT development strategy in place.[39] China's late start heightened the concern among Chinese government researchers that China was already lagging behind the IoT capabilities of other countries, despite the country's achievements in a series of demonstration projects in IoT application areas like smart meters, transportation, logistics, smart homes, industrial automation, health care, financial services, public safety, and agriculture.[40] MIIT's 12th Five Year Plan Development Plan for the Internet of Things outlined several shortcomings of the Chinese IoT industry, noting that Chinese IoT utilization was relatively low both in terms of volume and scale, that the industry lacked any leading IoT-specific companies, and that "big gaps" remained between China and other countries in core IoT technologies and high-end IoT products.[41] As such, China's policies towards IoT development reflected the perception that it urgently needed to prevent other countries from establishing or widening their leads in IoT capabilities.

Scientific and Technological Innovation in the Context of Chinese Grand Strategy

In a 2011 article in which Ministry of Finance officials offered a basic primer on IoT and its importance, they argued that developing IoT technology and a strong Chinese IoT industry is "an urgent requirement for achieving indigenously controlled technology and protecting national security" (是实现技术自主可控、保障国家安全的迫切需要), and that "[O]ver dependence on foreign technology is a major risk to Chinese national security."[42] As this suggests, China's prioritization of IoT development has taken place in an environment in which Chinese leaders view scientific and technological innovation as a decisive strategic resource that drives national productivity and a country's overall strength, making it critical to China's security and its "rejuvenation" as a great power.[43] These beliefs continue to influence Chinese national strategy

[38] "物联网'十二五'发展规划》发布" [The 'Internet of Things 12th Five Year Plan Development Plan' is Released], Ministry of Industry and Information Technology, February 14, 2012, www.miit.gov.cn/n1146295/n1146562/n1146650/c3074283/content.html.

[39] Ma Xianwen 马先文, "标准落地力助产业链重塑, 物联网发展迈入全新轨道" [Standards Birth Helps Remold Industry Chains, the Internet of Things Moves onto a Completely New Track], 长江证券 *Changjiang Securities*, June 23, 2016, 13-14.

[40] [2011 White Paper on IoT], China Academy of Telecommunication Research of MIIT, 15-16.

[41] "物联网'十二五'发展规划》发布" [The 'Internet of Things 12th Five Year Plan Development Plan' is Released], Ministry of Industry and Information Technology, February 14, 2012, www.miit.gov.cn/n1146295/n1146562/n1146650/c3074283/content.html.

[42] "财政部就'物联网发展专项资金管理暂行办法'答问" [The Ministry of Finance Answers Questions About the 'Interim Methods for Managing the Special Projects Fund for IoT Development], Ministry of Industry and Information Technology, April 19, 2011, http://miit.gov.cn/n1146290/n1146402/n1146455/c3226838/content.html.

[43] Zheng Wang, "Not Rising, But Rejuvenating: The 'Chinese Dream'," *The Diplomat*, February 5, 2013, http://thediplomat.com/2013/02/chinese-dream-draft/; "Xi Jinping's Vision: Chasing the Chinese Dream," *The*

and the government's approach to technology development. As the Ministry of Science and Technology's (MOST) background briefing on the State Council's 2016 "Outline of the National Strategy of Innovation-Driven Development" (国家创新驱动发展战略纲要) stated:

> The strength of a nation is ultimately determined by its ability to innovate. In the modern history, the center of the world economy has shifted several times, yet there has been a clear logic behind it. That is, the scientific center has always been a major driving force behind the geographic shift of economic center [sic]. Places where cutting-edge technologies and high-end professionals flock are always the ones that seize the command heights and boast economic competitiveness. More than ever before, China needs the power of scientific innovation to realize her dream of national rejuvenation. China cannot afford any delay in the implementation of the strategy of innovation-driven development. [44]

Throughout his tenure as CCP chairman, Xi Jinping has demonstrated his support for this philosophy and has repeatedly stressed China's need to become a leader in technology development. As he warned in 2016, "The situation that our country is under others' control in core technologies of key fields has not changed fundamentally, and the country's S&T foundation remains weak." [45] China's strategic imperative to innovate gives its focus on promoting an indigenous IoT industry an added urgency and colors its perceptions of global competition within the industry. As the aforementioned MOST background briefing on the "Outline of the National Strategy of Innovation-Driven Development" argued,

> [Technology innovations] generate unprecedented momentum for socio-economic development and trigger profound economic and industrial restructuring. They are the key factors for China's growth and increased international competitiveness. China now faces a rare historic opportunity for a quantum leap and also a risk of having existing gaps further widened. Only with a stronger sense of crisis and readiness to break new ground can China keep up with the world's development and take the initiative of development in her own hands. [46]

In his Work Report at the 2016 National People's Congress, Premier Li Keqiang explicitly linked technologies like the IoT to this innovation imperative as part of the government's drive to make China a global economic leader. [47]

Economist, May 4, 2013, www.economist.com/news/briefing/21577063-chinas-new-leader-has-been-quick-consolidate-his-power-what-does-he-now-want-his.

[44] Ministry of Science and Technology of the People's Republic of China, "Outline of the National Strategy of Innovation-Driven Development–Background Briefing," china.com, May 23, 2016, www.china.com.cn/zhibo/zhuanti/ch-xinwen/2016-05/23/content_38515829.htm.

[45] "President Xi Says China Faces Major Science, Technology 'Bottleneck'," Xinhua, June 1, 2016, http://news.xinhuanet.com/english/2016-06/01/c_135402671.htm.

[46] Ministry of Science and Technology of the People's Republic of China, "Outline of the National Strategy of Innovation-Driven Development–Background Briefing."

[47] Li Keqiang, "Report on the Work of the Government," Fourth Session of the 12th National People's Congress of the People's Republic of China (speech transcript), March 5, 2016, http://english.gov.cn/premier/news/2016/03/17/content_281475309417987.htm.

> Innovation is the primary driving force for development and must occupy a central place in China's development strategy, which is why we must implement a strategy of innovation-driven development. We should launch new national science and technology programs, build first-class national science centers and technological innovation hubs, help develop internationally competitive high-innovation enterprises, and establish pilot reform zones for all-round innovation. We should make consistent efforts to encourage the public to start businesses and make innovations. We should promote the extensive application of big data, cloud computing, and the Internet of Things. We need to move faster to transform China into a manufacturer of advanced and quality products and a country that is strong on intellectual property rights. We should strive to achieve major breakthroughs in basic research, applied research, and research in strategic and frontier fields by 2020.

Government Support for IoT Development

Once the government labeled the IoT a key strategic emerging industry in 2009, it rapidly became a core component of subsequent Chinese development plans, featuring in both IoT industry-specific development plans and as part of plans for other fields in which IoT plays an ancillary role, such as broadband networks and big data. A representative but not exhaustive list is included in Table 2. These plans guide, coordinate, and support IoT development and build up from a baseline of early stage technologies (sensors, chips, information security, and so on), to infrastructure and applications (logistics, agriculture, power grids, public security, transportation, medical treatment, and other uses).[48] They are also designed to target and remedy shortcomings and bottlenecks in the China's IoT industry's development, such as China's ongoing reliance on imports for key components like chips, sensors, and MEMS sensors. There are some discrepancies about the precise size of this dependence, but analysts agree that China still imports more than 80 percent of its advanced chip needs, roughly 60 percent of its sensors, and virtually all of its advanced MEMS sensors.[49] This is particularly troubling for the Chinese in an environment in which the United States may be less willing to trade these components, since Chinese reliance on U.S. imports, specifically, is particularly high in areas like chips.[50]

The earliest guidance documents were heavily influenced by the policy research contained in the "2011 IoT White Paper" (物联网白皮书 (2011 年)) produced by MIIT's China Academy of Telecommunication Research.[51] This White Paper provided a common understanding of the state

[48] "物联网'十二五'发展规划" (12th Five Year Plan Development Plan for the Internet of Things), Ministry of Industry and Information Technology of the People's Republic of China, February 14, 2012, http://politics.people.com.cn/GB/1027/17111472.html; [2011 White Paper on IoT], China Academy of Telecommunication Research of MIIT, 15-16.

[49] "物联新时代遭遇核心技术瓶颈 芯片等依赖进口" (The Internet of Things Era Encounters Core Technology Bottlenecks–Dependent on Imports for Chips and Other Technologies), *Economic Information Daily* (经济参考报), September 18, 2017, http://news.china.com.cn/2017-09/18/content_41602969.htm.

[50] "美国拿中兴 '开刀' 背后: 中国芯片 9 成依赖进口, 我们拿什么反抗?" (Behind the United States' 'Operation' on ZTE: China Relies on Imports for 90 Percent of its Chips, What Can We Resist?), *PE Daily*, April 17, 2018, http://pe.pedaily.cn/201804/430167.shtml.

[51] The China Academy of Telecommunication Research (电信研究院) is currently known as the China Academy of Information and Communications Technology (CAICT / 中国信息通信研究院), after a name change in 2014. "我

of domestic and international IoT development; described IoT architecture, technology systems, industrial systems, and resource systems; and analyzed the opportunities and challenges facing Chinese IoT development.[52]

The key managing department for IoT development has been MIIT, but the State Council and a host of other ministries have also provided guidance. In 2013, China established an IoT-focused inter-ministerial council (物联网发展部际联席会议) and expert advisory committee (物联网发展专家咨询委员会) to help coordinate between overlapping areas of responsibility.[53] At local levels, provincial and municipal governments have created their own IoT development plans,[54] and by 2015, more than 90 percent of China's provinces and municipalities listed the IoT as a pillar industry in their development plans.[55]

By 2015, IoT development had also been incorporated into broader government plans, including the "Made in China 2025" (**中国制造** 2025) plan issued by the State Council. "Made in China 2025" called for accelerated IoT technology research and expanded application, and referenced uses like smart manufacturing, smart home applications, and smart cars.[56] Other related plans issued domestic production targets that incentive further Chinese IoT development: for instance, the Made in China 2025 Key Area Technology Roadmap (《中国制造 2025》重点领域技术路线图) calls for China to increase domestic market share of autonomous manufacturing robots to 70 percent, partially autonomous vehicles to 60 percent, and smart manufacturing equipment to 50 percent by 2025.[57] While Made in China 2025 makes little explicit reference to IoT development, its broader goals are an indication of the priority that Beijing places upon future IoT applications.

院简介," China Academy of Information and Communications Technology, accessed July 17, 2018, www2.caict.ac.cn/wygk/.

[52] [2011 White Paper on IoT], China Academy of Telecommunication Research of MIIT; Li Renbo 李仁波, "业绩稳定增长，物联网发展迎来黄金时期" (With Stable Growth in Performance, Internet of Things Development Has Ushered in a Golden Age), 联讯证券 *Lianxun Securities*, May 8, 2018, 15.

[53] Ministry of Industry and Informatization Technology of the People's Republic of China, "信息通信行业发展规划（2016－2020 年）物联网分册" [Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum], January 17, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057674/n4704636/c5465552/part/5465569.doc.

[54] Zhu Qian [朱茜], "Summary and Interpretation of 2017 State, Provincial, and Municipal Internet of Things Policies" [2017 年国家级个省市物联网政策汇总及解读], December 31, 2017, www.qianzhan.com/analyst/detail/220/171229-0b94cd33.html.

[55] "How China is Scaling the Internet of Things," GSMA Connected Living Program, July 9, 2015, https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf.

[56] "**中国制造** 2025 [Made in China 2025]," State Council of the People's Republic of China, May 8, 2015, http://www.miit.gov.cn/n973401/n1234620/n1234622/c4409653/content.html.

[57] "《中国制造 2025》重点领域技术路线图" (Made in China 2025 Key Area Technology Roadmap), Expert Commission for the Construction of a Manufacturing Superpower, October 29, 2015, http://www.cae.cn/cae/html/files/2015-10/29/20151029105822561730637.pdf.

Table 2: IoT-Related Development Plans, 2010-2017

Issuing Date	Name of Plan	Function and Highlights	Issuing Agency
October 2010	Decision on Accelerating the Cultivation and Development of Strategic New Emerging Industries 《关于加快培育和发展战略性新兴产业的决定》	Highlights key industries (including the emerging IoT industry) and outlines approaches to cultivate and accelerate the development of these industries.[58]	State Council
April 2011	Methods for Internet of Things Special Fund Management 《物联网专项基金管理办法》	Issues a series of specialized funds meant to accelerate the application and development of the Internet of Things.[59]	Ministry of Finance
February 2012	12th Five Year Plan Development Plan for the Internet of Things 《物联网'十二五'发展规划》	Identifies the Internet of Things as an economic and technological "strategic high ground" (战略制高点之), and lays out IoT investment for 2011-2015.[60]	MIIT
May 2012	Notice from the Office of the National Development and Reform Commission on Organizing and Implementing the 2012 Special Projects on Internet of Things Industrialization and Technology Research and Development 《国家发展改革委办公厅关于组织实施 2012 年物联网技术研发和产业化专项的通知》	Sets specific goals for developing IoT applications with major economic and social applications, and lays out reporting mechanisms and requirements for entities contributing to China's IoT development.[61]	NDRC

[58] "关于加快培育和发展战略性新兴产业的决定" [Decision on Accelerating the Cultivation and Development of Strategic New Emerging Industries], State Council of the People's Republic of China, October 18, 2010, http://www.gov.cn/zwgk/2010-10/18/content_1724848.htm.

[59] "投资要点" [Investment Focal Points], Fujian Province Trade Guidance Network, accessed September 6, 2018, http://tradeinservices.mofcom.gov.cn/article/difang/fujian/zhengcefg/201107/48451.html.

[60] "物联网'十二五'发展规划" [12th Five Year Plan Development Plan for the Internet of Things], Ministry of Industry and Information Technology of the People's Republic of China, February 14, 2012, http://www.miit.gov.cn/n1146295/n1146562/n1146650/c3074283/content.html.

[61] "国家发展改革委办公厅关于组织实施 2012 年物联网技术研发和产业化专项的通知" [Notice from the Office of the National Development and Reform Commission on Organizing and Implementing the 2012 Special Projects on Internet of Things Industrialization and Technology Research and Development], National Development and Reform Commission of the People's Republic of China, May 15, 2012, http://www.ndrc.gov.cn/zcfb/zcfbtz/201205/t20120518_480281.html.

July 2012	12th Five Year Plan Development Plan for National Strategic Emerging Industries 《“十二五” 国家战略性新兴产业发展规划》	Lays out the strategic rationale and guiding ideology informing the PRC’s investments in emerging technologies (including the IoT).[62]	State Council
August 2012	Wuxi National Sensor Network Innovation Exemplar Development Plan Outline (2012-2020) 《无锡国家传感网创新示范区发展规划纲要（2012—2020 年）》	Lays out a plan to use the city of Wuxi as a “national sensor network innovation zone” (国家传感网创新示范区), with the goal of using the city as a model for other cities in China seeking to “informationize” their economies. [63]	MIIT
September 2012	National Broadband Network Technology Development 12th Five Year Special Plan 《国家宽带网络科技发展 ‘十二五’ 专项规划》	Identifies IoT as a “strategic emerging industry,” (战略性新兴产业) alongside mobile internet and cloud computing and identifies the infrastructure requirements necessary to cultivate those technologies. [64]	MOST
February 2013	Guiding Opinion on Promoting the Orderly and Healthy Development of the Internet of Things 《关于推进物联网有序健康发展的指导意见》	Identifies the inability to domestically produce key technologies, poor device security, and the lack of a unified standards regime as weaknesses of China’s IoT economy.[65]	State Council
September 2013	Special Project Action Plan for Internet of Things Development 《物联网发展专项行动计划》	Lays out several specific goals for IoT development, and outlines a comprehensive series of sub-initiatives to be undertaken.[66]	NDRC, MIIT, MOST

[62] ““十二五” 国家战略性新兴产业发展规划” [12th Five Year Plan Development Plan for National Strategic Emerging Industries], State Council of the People’s Republic of China, July 9, 2012, http://www.gov.cn/zwgk/2012-07/20/content_2187770.htm.

[63] “无锡国家传感网创新示范区发展规划纲要 (2012-2020 年)” [Wuxi National Sensor Network Innovation Exemplar Development Plan Outline (2012-2020)], Ministry of Industry and Information Technology of the People’s Republic of China August 17, 2012, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057497/n3057507/c3630619/content.htm.

[64] “国家宽带网络科技发展 “十二五” 专项规划” [National Broadband Network Technology Development 12th Five Year Special Plan], Ministry of Science and Technology of the People’s Republic of China, September 18, 2012, http://www.most.gov.cn/tztg/201209/W020120918518757509871.doc.

[65] “关于推进物联网有序健康发展的指导意见” [Guiding Opinion on Promoting the Orderly and Healthy Development of the Internet of Things], State Council of the People’s Republic of China, February 5, 2013, http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm.

[66] “物联网发展专项行动计划” [Special Project Action Plan for Internet of Things Development], National Development and Reform Commission of the People’s Republic of China et al., September 5, 2013, http://www.chinatax.gov.cn/n810341/n810765/n812146/n812323/c1080708/part/1080710.pdf .

June 2014	National Integrated Circuit Industry Development Advancement Outline 《国家集成电路产业发展推进纲要》	Identifies IoT deployment as a major driver for integrated circuit development.[67]	MIIT
June 2014	MIIT’s Key Points for 2014 Internet of Things Work 《工业和信息化部 2014 年物联网工作要点》	Outlines a set of key IoT development goals for the year 2014.[68]	MIIT
September 2015	Outline on Promoting Big Data Development Actions 《关于促进大数据发展行动纲要》	Identifies IoT deployment as a major driver for big data development.[69]	State Council
November 2016	13th Five Year Plan Development Plan for Strategic New Emerging Industries 《‘十三五’国家战略性新兴产业发展规划》	Outlines China’s strategy for developing key industries (including the IoT) from 2016-2020.[70]	State Council
January 2017	Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum 《信息通信行业发展规划（2016－2020 年）物联网分册》	Guiding document for IoT industry development over the next five years calling for adjustments to adapt to an Internet of Everything era that has already begun.[71]	MIIT
June 2017	Notice on Comprehensively Advancing NB-IoT Development 《关于全面推进移动物联网(NB-IoT)建设发展的通知》	Calls for relevant provinces and municipalities to prepare NB-IoT for the 5G era, expand NB-IoT usage to smart cities, personal and home, and industry.[72]	MIIT

[67] “国家集成电路产业发展推进纲要” [National Integrated Circuit Industry Development Advancement Outline], Ministry of Industry and Information Technology of the People’s Republic of China, June 24, 2014, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757021/c3758335/content.html.

[68] “工业和信息化部 2014 年物联网工作要点” [Key Points for 2014 Internet of Things Work], Ministry of Industry and Information Technology of the People’s Republic of China, accessed September 4, 2018, http://www.gov.cn/zhengce/2014-05/21/5023657/files/de40b3afe788404ca6f8313837389442.pdf.

[69] “关于促进大数据发展行动纲要” [Outline on Promoting Big Data Development Actions], State Council of the People’s Republic of China, September 5, 2015, http://zfs.mep.gov.cn/fg/gwyw/201509/t20150917_309927.htm.

[70] “‘十三五’国家战略性新兴产业发展规划” [13th Five Year Plan Development Plan for Strategic New Emerging Industries], State Council of the People’s Republic of China, November 29, 2016, http://www.gov.cn/zhengce/content/2016-12/19/content_5150090.htm.

[71] “Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum,” Ministry of Industry and Information Technology of the People’s Republic of China.

[72] “工业和信息化部办公厅关于全面推进移动物联网（NB-IoT）建设发展的通知” [Notice on Comprehensively Advancing NB-IoT Development], Ministry of Industry and Information Technology of the People’s Republic of China, June 16, 2017, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5692719/content.html.

The two most substantive early planning documents for the IoT were MIIT's 12th Five Year Plan Development Plan for the Internet of Things, released in February 2012, and the "Notice from the Office of the National Development and Reform Commission on Organizing and Implementing the 2012 Special Projects on Internet of Things Industrialization and Technology Research and Development" released by the National Development and Reform Commission (NDRC / 国家发展和改革委员会) in May 2012, hereafter the "2012 Notice." While neither document set concrete financial targets, they guided the development of IoT infrastructure and set priorities for IoT policymaking, and many of the basic core tasks they identified remained in later IoT plans as items for further improvement.

To that end, both the 12th Five Year Plan Development Plan for the Internet of Things and the 2012 Notice stated that China should focus on:[73]

- Developing IoT application demonstration bases in key application areas;
- Achieving breakthroughs in the core technologies that are restricting further development of the IoT industry;
- Providing industrial support for scaled IoT development;
- Establishing basic IoT technology standards;
- Improving the IoT standards system;
- Resolving IoT testing and certification management issues;
- Strengthening the IoT industry's indigenous innovation ability; and
- Nurturing and developing a group of leading companies in both IoT technology R&D and IoT product and equipment manufacturing.

In an effort to foster growth and innovation in the country's IoT industry, the 12th Five Year Plan Development Plan for the Internet of Things called for nurturing a group of IoT integrated industrial clusters in east, central, and western China.[74] These clusters, launched in the Bohai Economic Rim (环渤海), Yangtze River Delta (长三角), Pan-Pearl River Delta (珠三角), and Central Western (中西部) regions, each specialized in different parts of the IoT development ecosystem, as depicted below in Table 3. The government's focus on industrial clusters reflected its belief that the geographic concentration of like industries could serve as centers of gravity for talent and resources and prevent uncoordinated investment, duplicated development, and too many like units competing against one another. MIIT also approved the creation of four IoT industrial demonstration bases: in Wuxi, Chongqing, Hangzhou, and Fuzhou.[75] Industrial demonstration bases were pilot programs for leading and driving the next wave of industrial development in China,

[73] "物联网'十二五'发展规划" (12th Five Year Plan Development Plan for the Internet of Things), Ministry of Industry and Information Technology, February 14, 2012, http://politics.people.com.cn/GB/1027/17111472.html; "国家发展改革委办公厅关于组织实施 2012 年物联网技术研发和产业化专项的通知" [Notice from the Office of the National Development and Reform Commission on Organizing and Implementing the 2012 Special Projects on Internet of Things Industrialization and Technology Research and Development], Office of the National Development and Reform Commission 国家发展和改革委员会办公厅, May 15, 2012, http://today.hit.edu.cn/uploadfiles/2012/5-21/物联网专项.pdf.

[74] "物联网'十二五'发展规划" 12th Five Year Plan Development Plan for the Internet of Things, Ministry of Industry and Information Technology of the People's Republic of China, February 14, 2012, http://politics.people.com.cn/GB/1027/17111472.html.

[75] "Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum," Ministry of Industry and Information Technology of the People's Republic of China.

focusing on specific industries. They were an attempt to improve on China's earlier high-tech park development model, which the government concluded had done little to create robust industrial networks precisely because they did not specialize in particular industries.[76]

Table 3: Regional IoT Industrial Clusters and their Focus, ca. 2016[77]

Region	IoT Industrial Focus
Yangtze River Delta (长三角)	Sensors; software development and systems integration
Pan-Pearl River Delta (珠三角)	Smart equipment manufacturing; software and systems integration; network operation services
Central Western (中西部)	Standardization, pilot programs, and applications
Bohai Economic Rim (环渤海)	Comprehensive IoT platforms

China's government quickly followed the 12th Five Year Plan Development Plan for the Internet of Things with a 2013 "Special Project Action Plan for Internet of Things Development" (物联网发展专项行动计划), hereafter the 2013 Special Project Action Plan,[78] which sought to coordinate the efforts of ten central ministries in developing the IoT industry.[79] It identified goals, tasks, and responsible departments covering ten separate areas of IoT development policy: top-level design, standards formation, technology R&D, application and promotion, industrial support, business models, safety, government support, laws and regulations, and workforce training.[80]

[76] Wang Liming and Sun Feng, "SME Cluster: A Study of High-Tech Parks in China" (paper presented at the Eighth West Lake International Conference on SMB [Small and Medium Business], November 2006), http://www.seiofbluemountain.com/search/detail.php?id=3120.

[77] Ma Xianwen, "Standards Birth Helps Remold Industry Chains," 13-14.

[78] "Special Project Action Plan for Internet of Things Development," National Development and Reform Commission of the People's Republic of China et al.

[79] "物联网发展专项行动计划牵头部门" [Leading Departments for the Special Project Action Plan for Internet of Things Development], National Development and Reform Commission of the People's Republic of China et al., September 5, 2013, http://www.chinatax.gov.cn/n810341/n810765/n812146/n812323/c1080708/part/1080709.pdf.

[80] "How China is Scaling the Internet of Things," GSMA Connected Living Program, July 2015, 8, https://www.gsma.com/newsroom/wp-content/uploads/16531-China-IoT-Report-LR.pdf.

The 2013 Special Project Action Plan, which was meant to be achieved by 2015, did not identify growth targets or other concrete metrics for progress. Instead, it identified the following top-line goals:[81]

- Improve mechanisms for IoT overall coordination;
- Begin to realize mutual coordination in IoT development between departments, industries, regions, and military and civilians;
- Begin to realize mutual coordination in the spread of IoT applications, technology R&D, setting IoT standards, creating supply chains, developing IoT infrastructure, ensuring IoT information security, and handling IoT spectrum resource allocation; and
- Form a basic coordinated, synergistic, and mutually supportive development effect in each segment of the IoT industry.

In accordance with its planning document guidelines, by 2014, the central government had selected 202 cities to pilot smart city projects, and Beijing, Shanghai, Guangzhou, Hangzhou, and other large cities have established extensive database and sensor networks to collect, store, and analyze information related to transportation, electricity, public safety, and environmental factors.[82]

Financial Support for the IoT Industry

The Chinese government's financial support for an indigenous IoT industry, at both central and lower levels, has been codified in the planning documents and guidance described in the previous section. The 12th Five Year Plan Development Plan for the Internet of Things, for example, directed the government to implement favorable tax policies for the IoT industry, increase the scale of funding for special projects supporting IoT development, increase the proportion of investment in IoT-related product commercialization, and encourage non-state investment in IoT-related areas.[83] The subsequent Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum included similar mandates. It called for the central government to increase its fiscal support for IoT, to support R&D and commercialization of key IoT technologies, to extend credit support for major IoT projects, to encourage private and venture capital investment in the IoT industry, and to encourage local governments to establish more IoT support funds.[84] In February 2013, the State Council released its "Guiding Opinion on Promoting the Orderly and Healthy Development of the Internet of Things" (关于推进物联网有序健康发展的指导意见), which included provisions calling for greater financial support for the IoT. According to the Guiding Opinion:

[81] [Special Project Action Plan for Internet of Things Development], National Development and Reform Commission of the People's Republic of China et al.

[82] "How China is Scaling the Internet of Things," GSMA Connected Living Program.

[83] "物联网'十二五'发展规划" (12th Five Year Plan Development Plan for the Internet of Things), Ministry of Industry and Information Technology, February 14, 2012, http://politics.people.com.cn/GB/1027/17111472.html

[84] "Information and Communication Industry Development Plan (2016–2020) Internet of Things Addendum," Ministry of Industry and Information Technology of the People's Republic of China.

> We should encourage investment from financial capital, venture capital, and private capital in IoT applications and the development of the IoT industry…. We should give priority credit support to significant IoT projects with strong drive and support, advanced technology, and clear advantages. We should actively support IoT companies at home and abroad with direct capital market financing. We should encourage the establishment of IoT equity investment funds, and establish a group of IoT entrepreneurial investment funds through the state strategic emerging industry venture capital plan.[85]

These directives reflected the Chinese leadership's belief in the indispensable role of the state as the lead investor in the development of new technologies.[86] As former Vice Minister of MIIT Xi Guohua stated in September 2014, "Government support is important because the IoT industry is still in its primary stage."[87]

The precise level of China's state financial support for IoT development is not readily available, but the government's ongoing commitment to IoT as a core technological priority makes it very likely that it has devoted substantial resources towards fostering its development. This support has included state-directed research funds, state-backed investment funds, government subsidies, and other awards. Some examples of these financial support vehicles are discussed in this section, but they represent only a small sample of the government's overall financial commitment to the IoT industry's development.

In 2011, MIIT and the Ministry of Finance created a Special Projects Fund for IoT Development (物联网发展专项资金), hereafter the "IoT Special Projects Fund," to support corporate IoT R&D initiatives.[88] The budget for the fund came directly from the Ministry of Finance, which dispensed this fund in the form of grants and discount loans.[89] In its first four years, the IoT Special Projects Fund spent an average of 500 million RMB (approx. $80 million) per annum, supporting more than 500 IoT-related R&D projects.[90] Some of the companies receiving support from the IoT

[85] "国务院关于推进物联网有序健康发展的指导意见" [The State Council's Guiding Opinion on Promoting the Orderly and Healthy Development of the Internet of Things], State Council of the People's Republic of China, February 5, 2013, http://www.gov.cn/zwgk/2013-02/17/content_2333141.htm.

[86] Tai Ming Cheung, "China's Rise as a Global Military Technological Power: Geo-Strategic and Geo-Economic Implications," February 19, 2018, https://chairestrategique.univ-paris1.fr/fileadmin/chairestrategiesorbonne/Conference_2018/Documents/Tai_Ming_Cheung_-_Chaire_des_Grands_Enjeux_Strategiques_2018.pdf

[87] "How China is Scaling the Internet of Things," GSMA Connected Living Program.

[88] Zong Xiuqian 宗秀倩, "工信部拟明年设 5 亿专项资金支持物联网发展" [Next Year MIIT Intends to Invest 500 million RMB in the Special Projects Fund for IoT Development], Tencent Science and Technology 腾讯科技, December 21, 2012, http://tech.qq.com/a/20121221/000103.htm.

[89] "物联网发展专项资金管理暂行办法" [Interim Methods for Management of the Special Projects Fund for IoT Development], Ministry of Industry and Information Technology and Ministry of Finance, August 17, 2012, www.hngidz.com/?p=813.

[90] Yang Yanci 杨颜慈 and Sun Quan 孙权, "国家工信部：中国物联网产业规模达 7500 亿 互联网巨头成重要力量" [Ministry of Industry and Information Technology: The Scale of China's IoT Industry has Reached 750 Billion RMB, Internet Giants Have Become an Important Force], China News Service, October 29, 2016, http://www.chinanews.com/cj/2016/10-29/8047350.shtml; "工信部公示物联网发展专项资金拟支持 101 项目" [The Ministry of Industry and Information Technology's Special Projects Fund for IoT Development Plans to Support 101 Projects], Sina Finance, June 18, 2014, http://finance.sina.com.cn/china/bwdt/20140618/104019447599.shtml; Zong Xiuqian 宗秀倩, "工信部拟明年设 5

Special Projects Fund included Hisense (a major state-owned appliance and electronics manufacturer), Sichuan Changhong Electric Co., Ltd. (a consumer electronics conglomerate), and China Telecom Co., Ltd. (a subsidiary of China Telecom Corporation, the state-owned Chinese telecommunications company).[91] China also utilized broader investment vehicles, like the 100 billion RMB (approx. $14.6 billion) China Internet Investment Fund (CIIF / 中国互联网投资基金), to promote IoT and related industries.[92]

The central government also funded academic research on the IoT through the National High-Tech R&D Program (863 Program), the National Basic Research Program of China (973 Program), the National Science and Technology Support Program, and the National Natural Science Fund– funding programs managed by the Ministry of Science and Technology and the National Natural Science Foundation of China. The financial extent of this support is unknown, but a review of IoT-related articles published between 2008 and 2017 on the China National Knowledge Infrastructure (CNKI) database identified more than two thousand publications that were the product of research supported by one of these plans.[93]

Media reports and CCP documents suggest that a substantial portion of government funding for IoT innovation is provided at the provincial level and below. The Jiangsu provincial government was an early example of this, as by early 2010 it had already arranged 180 million RMB (approx. $26.3 million) in subsidies for local R&D in IoT-related technologies.[94] Provincial and municipal governments also created their own IoT development funds—such as the Anhui Special Projects Fund for IoT Development and the Fujian Special Projects Fund for IoT Development—to support R&D efforts within their jurisdictions.[95] These efforts began as early as 2010, when the Shanghai IoT Entrepreneurial Investment Fund (上海物联网创业投资基金) launched with 408.5 million RMB (approx. $62 million) in funding, backed by the CAS Shanghai Institute of Microsystem and

亿专项资金支持物联网发展" [Next Year MIIT Intends to Invest 500 million RMB in the Special Projects Fund for IoT Development], Tencent Science and Technology 腾讯科技, December 21, 2012, http://tech.qq.com/a/20121221/000103.htm. The U.S. dollar approximation is based on the January 1, 2012, January 1, 2013, and January 1, 2014 exchange rates. "Current and Historical Rate Tables," XE, accessed July 18, 2018, www.xe.com/currencytables/?from=CNY&date=2012-01-01; www.xe.com/currencytables/?from=CNY&date=2013-01-01; www.xe.com/currencytables/?from=CNY&date=2014-01-01.

[91] "2013 年物联网发展专项资金拟支持项目表" [Table of 2013 Projects to be Funded by the Planned Special Projects Fund for IoT Development], Ministry of Industry and Information Technology, accessed July 18, 2018, www.miit.gov.cn/n1146285/n1146352/n3054355/n3057497/n3057507/c3630670/part/3630671.xls.

[92] "中国互联网投资基金成立，总规模 1000 亿元人民币，首期 300 亿已到位" (China Internet Investment Fund Launches as a 100 Billion RMB Fund, with a First Phase of 30 billion RMB Already in Place), *PE Daily*, January 22, 2017, https://pe.pedaily.cn/201701/20170122408334.shtml; "China Launches $14.6b Internet Investment Fund," Xinhua (新华), January 23, 2017, http://english.gov.cn/news/top_news/2017/01/23/content_281475549246254.htm.

[93] Database results acquired using "IoT" (物联网) as a keyword in either article title or abstract, from the period 2008-2017. Accessed July 19, 2018, www.cnki.net.

[94] Zhang Zhanpeng 张展鹏, "江苏已资助 1.8 亿元发展物联网" (Jiangsu Has Already Subsidized 180 Million RMB for the Development of IoT), Tencent Technology (腾讯科技), March 31, 2010, http://tech.qq.com/a/20100331/000324.htm.

[95] "安徽省物联网发展专项资金" [Anhui Special Projects Fund for IoT Development], Anhui Wotao, accessed July 19, 2018, http://wotaochina.com/info.asp?second_id=3014; "转发关于做好 2012 年福建省物联网发展专项资金项目申报工作的通知" [Forwarded Notice Concerning Properly Applying for the 2012 Fujian Special Projects Fund for IoT Development], Fujian Internet of Things Alliance, March 31, 2012, www.fjitc.com/fjiota/index.php/news/2012-04-11-03-32-15/135-2012.

Information Technology (中科院上海微系统所与信息技术研究所) and the Jiading District government (嘉定区政府).[96] Examples of local government support also included the Wuxi Special Projects Fund for IoT Development (无锡市物联网发展专项资金) and the Xi'an Special Projects Fund for IoT Development (西安市物联网发展专项资金).[97] In addition, local governments supported IoT development under the auspices of broader investment funds, such as Shanghai's Special Projects Fund for Strategic Emerging Industries (上海市战略性新兴产业发展专项资金), which contained provisions for financing new uses for IoT technologies.[98]

These sentiments were echoed in the September 2013 Special Project Action Plan referenced above, which called for the NDRC and Ministry of Finance to oversee the creation of IoT venture capital funds and to steer IoT investment funds towards promising small- and medium-sized IoT companies that have mastered key technologies or developed innovative IoT business models.[99] The first public-private IoT venture capital fund of this kind was the 250 million RMB (approx. $40 million) Yongyi IoT Industry Fund (永益物联网产业基金), launched in December 2011, which combined public financing from the Ministry of Finance and the Fujian provincial government with investment from individuals and private industry.[100]

IoT investment continues to feature in IoT planning documents, like MIIT's "Internet of Things Development Plan (2016–2020)," released in January 2017. It called for setting up IoT-related venture capital funds as part of an effort to spur greater IoT innovation, and for stronger links between financial capital and the IoT industry. It also encouraged greater venture capital investment support for IoT industry development.[101]That same year, the government's annual investment in IoT reached 10 billion RMB (approx. $1.6 billion), reflecting the operationalization

[96] "创投基金" [Venture Capital Fund], Simi Holdings 上海新微科技集团, accessed May 18, 2018, http://www.simicholdings.com/venture/ventureInvestment/6cb50e88fd9b44aeab7a82905a74048d.

[97] "物联网 关于发布 2015 年度无锡市物联网发展专项资金项目申报指南" [IoT - Concerning the Release of 2015 Filing Guidelines for Wuxi's Special Projects Fund for IoT Development], Wuxi Huishan Software Outsourcing Park, August 21, 2015, http://wxo-park.com/index.php?g=&m=article&a=index&id=112; "西安市征集物联网发展专项资金项目" [Xian Collects Projects for the Special Projects Fund for IoT Development], IoT World, May 16, 2014, www.iotworld.com.cn/html/News/201405/9fb2b40b30bf04e5.shtml.

[98] "上海市战略性新兴产业发展专项资金" [Shanghai Special Projects Fund for Strategic Emerging Industries], Chinese Government Network, September 26, 2012, www.gov.cn/zhengce/2012-09/26/5023746/files/5c07b748c14142dda10e3e2dc4a25d5f.doc.

[99] [Internet of Things Development Special Action Plan], National Development and Reform Commission of the People's Republic of China et al.

[100] "物联网基金" [IoT Fund], Fujian Newland Computer Co., Ltd., accessed July 20, 2018, www.newland.com.cn/zgs2.html; "福建永益物联网产业创业投资有限公司" [Fujian Yongyi IoT Industry Innovation Investment Co., Ltd.], Fujian Strait Development of IoT Applications Center, March 22, 2017, www.iot-hx.com/index.php?s=news&c=show&id=74; "福建新大陆电脑股份有限公司关于出资成立"福建永益物联网产业创业投资有限公司"的公告" [Notice from Fujian Newland Computer Co., Ltd. Concerning Funding to Establish 'Fujian Yongyi IoT Industry Innovation Investment Co., Ltd.'], December 20, 2011, www.cninfo.com.cn/finalpage/2011-12-20/60343606.PDF.

[101] "信息通信行业发展规划 (2016－2020 年) 物联网分册" Information and Communications Industry Development Plan (2016–2020), [Internet of Things Addendum], Ministry of Industry and Information Technology of the People's Republic of China, January 17, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057674/n4704636/c5465552/part/5465569.doc.

of Party directives to increase investments in the IoT.[102]In some cases, money from national-level investment funds has been re-directed towards more IoT investment in an attempt not only to encourage IoT development, but also to implement structural reform of China's economy. One prominent example of this is the partial re-orientation of the 350 billion RMB (approx. $52 billion) China Structural Reform Fund Corporation (中国国有企业结构调整基金股份有限公司). Originally set up in September 2016 as a direct investment vehicle to funnel money towards supporting state enterprises, by September 2017, it was announced that the corporation would direct funding towards more IoT investment in accordance with the "Made in China 2025" Plan.[103]

Reports of new IoT investment vehicles have rapidly increased over the last two years, particularly at the local level. A second phase of the Shanghai Internet of Things Venture Capital Fund (上海物联网二期创业投资基金合伙企业) launched in Shanghai in 2016,[104] and in 2017, Guangdong province announced a joint investment fund between Nokia and Shanghai Bei'er (上海贝尔) focused on IoT spending and the 5G infrastructure needed to back it.[105]

Local IoT investment is likely to remain a favored tool for accelerating IoT development for the CCP into the foreseeable future. A March 2017 document issued by the Communist Party Committee of Wuxi City (中共无锡市委) revealed that investment at the municipal level would continue to use monetary awards and government subsidies to construct new IoT investment funds and expand the scale of existing IoT investment vehicles.[106] True to their word, Wuxi officials announced the formation of a new 5 billion RMB IoT industry fund ($766.1 million) six months after the March 2017 Party document was issued.[107] Wuxi is an especially prominent location for IoT development, serving as the sole designated "innovation exemplar district" (创新示范区), or demonstration ground, from 2012 to 2020.[108]

[102] "How China is Scaling the Internet of Things," GSMA Connected Living Program, 8. The U.S. dollar approximation is based on the December 31, 2014 exchange rate of 1 RMB to $0.1611169372. "Current and Historical Rate Tables," XE, accessed July 13, 2018, www.xe.com/currencytables/?from=CNY&date=2014-12-31.

[103] Liu Zhengning 刘政宁, ed., "结构调整基金成国企改革重要推手" [Structural Reform Fund Becomes Important Driver of State-Owned Enterprise Reform], *经济日报 Economic Daily*, September 20, 2017, http://cq.people.com.cn/GB/365412/news/2017920/2017920105545274335.htm.

[104] "上海物联网二期创业投资基金合伙企业 (有限合伙)" [Shanghai IoT Second Round Innovation Investment Fund], accessed May 18, 2018, https://www.qichacha.com/firm_f5d58264a5a35f0fb6c92ba14cb9e673.html.

[105] "诺基亚和上海贝尔发布物联网战略重心 成立投资基金" [Nokia and Shanghai Bei'er Announce IoT Strategic Focus, Form Investment Fund], Guangdong Province Go-Global Department of Commerce Public Service Platform 广东省走出去公共服务信息平台, June 5, 2017, http://go.gdcom.gov.cn/article.php?typeid=10&contentId=4306.

[106] "关于无锡国家传感网创新示范区建设 (2017—2020 年) 实施意见" [Implementation Opinion Regarding Wuxi National Sensor Network Innovation Exemplar Construction (2017-2020)], Chinese Communist Party Committee of Wuxi City, March 20, 2017, http://www.wuxi.gov.cn/uploadfiles/201704/01/2017040113263886795157.doc.

[107] Zhang Xin 张鑫 and Chen Tianyuan 陈天源, eds., "无锡成立 50 亿元物联网产业基金引导行业发展" [Wuxi Forms 5 Billion Yuan Internet of Things Industry Fund to Usher in Industry Development], *人民网-江苏频道 People's Daily Jiangsu Channel*, September 11, 2017, http://js.people.com.cn/n2/2017/0911/c360301-30720833.html. Currency exchange information based on September 11, 2017 exchange rate of $1 to 0.1532244503 RMB, accessed May 18, 2018, https://www.xe.com/currencytables/?from=CNY&date=2017-09-11

[108] "国务院关于无锡国家传感网创新示范区发展规划纲要 (2012—2020 年) 的批复" [State Council Outline Regarding Development of Wuxi National Sensor Network Innovation Exemplar (2012–2020)], Ministry of Industry and Information Technology of the People's Republic of China, August 13, 2012, http://www.gov.cn/zwgk/2012-08/13/content_2203167.htm.

Finally, it is worth noting that some local IoT investment programs have directly invested in military-civilian fusion (军民融合) efforts, commonly referred to as 'civil-military integration' (CMI), focusing on the development of IoT technology in areas with potential dual-use applications.[109] For example, the Wuxi Aerospace National Elite Internet of Things Stock Investment Fund (无锡航天国华物联网投资企业)[110] was established in 2012 with 308 million RMB (approx. $50 million) of registered capital. It counted China Aerospace Investment Holdings Ltd. (CAIH / 航天投资控股有限公司)–an investment arm of the defense conglomerate China Aerospace Science and Technology Corporation (CASC)–and the state and defense industry-backed Guo Hua Civil-Military Integration Industrial Development Fund (国华军民融合产业发展基金) as two of its four primary investors, and these organizations have explicitly pursued investments to support China's defense technology development.[111]

The Current State of China's IoT Development

In 2010, shortly after it identified the IoT industry as one of its core development priorities, China officially estimated that the size of its IoT industry was "close to" 200 billion RMB (接近 2000 亿元, or approximately $29.25 billion).[112] From this baseline, China's IoT industry grew rapidly, featuring a compound annual growth rate of more than 25 percent over the course of the 12th Five Year Plan (2011-2015), so that its market size topped 900 billion RMB (approx. $131.6 billion)

[109] Civil-military integration refers to China's efforts to break down the barriers that previously kept its military and defense industrial systems separate from the broader civilian economy. It seeks to merge civilian and military development resources into a combined system that pursues substantially more cost-effective coordinated development and resource sharing. Daniel Alderman, Lisa Crawford, Brian Lafferty, and Aaron Shraberg, "The Rise of Chinese Civil-Military Integration," in Tai Ming Cheung, ed., *Forging China's Military Might* (Baltimore, MD: Johns Hopkins University Press, 2014), 109-135.

[110] The fund was formerly known as the Wuxi Aerospace High-Capability Internet of Things Stock Investment Fund (无锡航天高能物联网股权投资基金企业). See "航天科技基金孵化平台：促进航天技术应用产业化" [Aerospace Technology Funds Incubation Platforms: Promoting Aerospace Technology Application Production], China Aerospace Science and Technology Corporation (CASC), April 20, 2016, http://www.miit.gov.cn/n973401/n4702337/n4714008/c4732419/content.html.

[111] "无锡航天国华物联网投资企业 (有限合伙)" [Wuxi Aerospace National Elite Internet of Things Stock Investment Fund], accessed May 18, 2018, https://www.qichacha.com/firm_60ebb85af2d23be369a31b4995796111.html; "无锡航天国华物联网投资企业(有限合伙)" [Wuxi Aerospace Elite Internet of Things Stock Investment Fund], November 22, 2012, http://caih.spacechina.com/n9467/n9551/n9836/124001.html; "公司简介" [Company Introduction], accessed September 4, 2018, www.caih.cn/n9467/n9491/index.html; "国华军民融合产业发展基金创立 - 首期规模 302 亿" [The Guo Hua Civil-Military Integration Industrial Development Fund is Founded as a 30.2 Billion RMB Fund], September 7, 2016, www.gov.cn/xinwen/2016-09/07/content_5106111.htm; Li Jiayi 李佳懿, "航天物联网基金增资无锡航天飞邻 980 万元" [Aerospace IoT Fund Invests 9.8 Million RMB in Wuxi Aerospace Feilin], *中国航天报 China Aerospace Report*, January 26, 2015, http://www.spacechina.com/n25../n144/n206/n220/c834918/content.html. See also Li Jiayi 李佳懿, "航天物联网基金增资无锡航天飞邻 980 万元" [Aerospace IoT Fund Invests 9.8 Million RMB in Wuxi Aerospace Feilin], *中国航天报 China Aerospace Report*, January 26, 2015, http://www.spacechina.com/n25../n144/n206/n220/c834918/content.html.

[112] "《物联网'十二五'发展规划》发布" [The 'Internet of Things 12th Five Year Plan Development Plan' is Released], Ministry of Industry and Information Technology, February 14, 2012, http://www.miit.gov.cn/n1146295/n1146562/n1146650/c3074283/content.html.

by the end of 2016.[113] By the start of 2017, analysts from MIIT's China Academy of Information and Communications Technology (CAICT / 中国信息通信研究院) were stating that IoT had established itself as the current (rather than the next) generation technology in the information and communications technology (ICT) industry. In their assessment, the conditions for wide-scale IoT industry development were quickly falling into place, and the next two to three years would be a critical period, featuring a new wave of development led by smart upgrades in traditional industries and large-scale adoption of IoT in the consumer market.[114] This growth was fueled by dramatically lower costs for sensors and bandwidth, as well as the development of cloud computing.[115]

MIIT planning documents have also noted that China has already developed a relatively complete IoT industry supply chain, with representative enterprises in chips, components, devices, software, systems integration, operators, and applied services.[116] These include HiSilicon and ZTE in chips, Huawei, ZTE, and DTmobile in system equipment, and China Mobile, China Unicom, and China Telecom as operators.[117] By 2017, China established itself as the world's largest machine-to-machine (M2M) market, with more than 100 million cellular M2M connections,[118] and it staked out a strong early position in 5G market capabilities. In addition, advances in IoT technologies were also opening up significant development space for a host of new or more expanded IoT applications.[119] According to analyst forecasts, by 2020, the five largest global IoT application areas in terms of market share were expected to be:[120]

- Smart cities, which enable real-time data collection networks to monitor activity above ground (public utilities, the flow of people and traffic), below ground (pipeline operations), in air (air quality), and in water (water quality);
- Industrial IoT, which helps to optimize operations, enable predictive maintenance, and monitor performance of products;
- Medical IoT, which facilitates patient monitoring, optimizes patient care, and archives clinical data that can help drive future innovations in health care

[113] Zhu Qian 朱茜, "2017 年国家级个省市物联网政策汇总及解读" [Summary and Interpretation of 2017 State, Provincial, and Municipal Internet of Things Policies], December 31, 2017, www.qianzhan.com/analyst/detail/220/171229-0b94cd33.html; "信息通信行业发展规划(2016－2020 年)物联网分册" Information and Communications Industry Development Plan (2016–2020), [Internet of Things Addendum], Ministry of Industry and Information Technology of the People's Republic of China, January 17, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057674/n4704636/c5465552/part/5465569.doc

[114] "物联网白皮书(2016 年)" [Internet of Things White Paper (2016)], 中国信息通信研究院 (China Academy of Information and Communications Technology), December 2016.

[115] Liu Rong 刘荣 and Wu Dan 吴丹, "物联网设备专题研究 - 上篇" (Special Report on Internet of Things Devices–Part One), *招商证券 China Merchants Securities (CMS)*, July 16, 2018, 4-5.

[116] Liu and Wu, "Special Report on Internet of Things Devices–Part One," 8; "信息通信行业发展规划 (2016－2020 年) 物联网分册" [Information and Communications Industry Development Plan (2016–2020), Internet of Things Addendum], Ministry of Industry and Information Technology of the People's Republic of China, January 17, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057674/n4704636/c5465552/part/5465569.doc.

[117] Bian Tiecheng 边铁城, Cai Jing 蔡靖, and Yuan Haiyu 袁海宇, "5G 推动万物互联，物联网终端市场首先启动" [5G Promotes the Internet of Everything, Initial Start for the Internet of Things Terminal Market], *信达证券 Cinda Securities*, February 9, 2017, 9.

[118] M2M refers to the number of machine-to-machine connections, which serves as a metric for the size of a country's IoT industry.

[119] [Internet of Things White Paper (2016)], (China Academy of Information and Communications Technology).

[120] Liu and Wu, (Special Report on Internet of Things Devices–Part One), 8.

- Smart homes, which use IoT technologies to sense and respond to activity within a home, monitor home security, and provide remote control of home appliances;
- Smart cars, where IoT facilitates vehicle-to-everything (V2X) technologies built on vehicle-to-vehicle, vehicle-to-road, vehicle-to-person, vehicle-to-cloud services, and vehicle-to-device connections.

China's short term forecasts for its IoT market are bullish, with analysts forecasting that it will be worth 1.8 trillion RMB (approx. $264 billion) by 2020, and predicting the quick emergence of the "Internet of Everything" (IoE / 万物互联) era once IoT adoption hits critical mass.[121] These forecasts are already higher than the 2020 growth target set by MIIT in the "Internet of Things Addendum" to its "Information and Communications Industry Development Plan (2016–2020)," which called for China's IoT market size to grow past 1.5 trillion RMB (approx. $220 billion) by 2020.[122] It is worth noting that this plan marked the first time that one of China's national IoT planning documents set a firm target for overall growth in the industry, in contrast to earlier planning documents, which focused exclusively on developing IoT infrastructure.

MIIT's "Internet of Things Addendum," which effectively serves as the 13th Five Year Plan (2016-2020) guidance for the industry, also set a number of broad development goals for the IoT, such as creating a basic, internationally competitive IoT industrial supply chain, showing "significant improvement" (显著提高) in IoT technology R&D and innovation, and "basically forming" (基本成型) an IoT system with "ubiquitous security" (泛在安全). Some of the other targets it set included:[123]

- <u>Technology innovation</u>: Achieve "clear breakthroughs" in IoT network architecture, sensor technology, IoT operating systems, and security;
- <u>Standards</u>: Formulate 200 or more national and industry standards for IoT, and gradually improve the IoT standards system so that it can satisfy the requirements for IoT industrialization and IoT applications at scale;
- <u>Applications</u>: Promote a group of integrated application solutions in industrial manufacturing and modern agriculture, as well as in consumer areas like smart homes and medical services, and form a group of scaled applications. Create cross-domain data sharing mechanisms in areas like smart city development and management;
- <u>Industrial upgrades</u>: Create 10 distinct IoT industry clusters, cultivate and develop roughly 200 backbone IoT companies that are each valued at more than 1 billion RMB (approx. $147 million), develop a group of "specialized and innovative" small- and medium-sized enterprises, create a group of IoT public service platforms that offer broad coverage and strong industry support, and build an internationally competitive IoT industry;
- <u>Security protection</u>: Achieve breakthroughs in R&D for IoT core security technologies and specialized security products, formulate a group of national and industrial standards for

[121] Liu and Wu, (Special Report on Internet of Things Devices – Part One), 8; [Internet of Things White Paper (2016)], (China Academy of Information and Communications Technology).

[122] "信息通信行业发展规划 (2016－2020 年) 物联网分册" Information and Communications Industry Development Plan (2016–2020), [Internet of Things Addendum], Ministry of Industry and Information Technology of the People's Republic of China, January 17, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057674/n4704636/c5465552/part/5465569.doc.

[123] Ministry of Industry and Information Technology of the People's Republic of China, "Information and Communications Industry Development Plan (2016–2020)", [Internet of Things Addendum].

> IoT security, establish basic mechanisms for IoT security assessment, risk assessment, security prevention, and emergency response, and significantly strengthen security capacity in IoT infrastructure, major systems, and important information.

In addition to these goals, China has become particularly invested in establishing Narrowband IoT (NB-IoT), a low-power and low-bandwidth networking technology that transmits on unused frequencies,[124] as the dominant LPWAN technology standard in China. China's preferred NB-IoT solution is competing against Sigfox (developed in France) and LoRa (also developed in France, but subsequently bought by Semtech, a U.S. company).[125] This effort has been led both by the Chinese government and China's three telecom operators. On the government side, in 2017, MIIT released the "Notice on Comprehensively Advancing NB-IoT Development," hereafter the "2017 Notice," which called for deploying 400,000 base stations by the end of 2017 to extend NB-IoT coverage to provincial capitals and the municipalities under the direct administration of the central government (e.g., Beijing, Shanghai), with a goal of deploying 1.5 million base stations in 2020 that would provide complete NB-IoT coverage within China. The 2017 Notice also set a target of 20 million NB-IoT-based M2M connections by the end of 2017, with a goal of 600 million M2M connections by 2020.[126]

China's main telecom operators have also implemented their own NB-IoT development strategies, based in part on projections that by 2020 roughly 60 percent of all M2M and IoT applications (e.g., smart cities, smart agriculture) will require low data rate transmission.[127] In terms of deployment, China Telecom announced in May 2017 that it had upgraded 310,000 NB-IoT base stations and had created the broadest coverage NB-IoT network in the world. China Unicom announced in April 2018 that it had deployed more than 300,000 NB-IoT base stations and had achieved basic coverage for the entire country. Finally, China Mobile announced in December 2017 that it had completed 120,000 NB-IoT base stations.[128] In total, China Mobile, China Telecom, and China Unicom have deployed or upgraded 710,000 NB-IoT base stations.

Problems with IoT Development

Chinese government research organizations have produced annual studies of the IOT industry's weaknesses in order to guide policymaking, and they offer authoritative assessments of the barriers that continue to serve as a drag on the industry's growth. Notably, even as the industry has grown and to some degree matured, many of the problems these annual studies have highlighted have persisted, despite some incremental progress in fixing them. For example, the 2014 White Paper produced by the MIIT's China Academy of Telecommunications Research (工业和信息化部电

[124] Brian Ray, "What is Narrowband IoT (NB-IoT)? Explanation and 5 Business Benefits," IoT For All, May 9, 2017, https://www.iotforall.com/what-is-narrowband-iot-nb-iot/.

[125] Yu Haining 于海宁, "物联网深度报告: 2018, 从供需结构中寻找确定性" (In-Depth Report on the Internet of Things: Finding Certainty in the Supply and Demand Structure, 2018), *长江证券 Changjiang Securities*, June 2, 2018, 7-8.

[126] "工业和信息化部办公厅关于全面推进移动物联网（NB-IoT）建设发展的通知" (Ministry of Industry and Information Technology General Office Concerning the 'Notice on Comprehensively Advancing NB-IoT Development'), Ministry of Industry and Information Technology, June 16, 2017, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5692719/content.html.

[127] Liu and Wu, (Special Report on Internet of Things Devices–Part One), 17.

[128] Yu Haining (In-Depth Report on the Internet of Things), 13.

信研究院) identified three key impediments to IoT growth.[129] First, it stated that the supply chain for China's IoT industry was highly decentralized and comprised of many small- and medium-sized enterprises. The absence of dominant industry leaders meant that despite rapid growth, the industry as a whole was not achieving economies of scale. Thus the basic costs of deploying IoT solutions to various applications remained high, hindering IoT's broader adoption.[130] The White Paper contrasted the state of China's IoT market with that of China's mobile internet market, which had produced a limited number of large enterprises that were able to exercise leadership within the industry and "act cohesively at home and abroad."[131]

Second, the 2014 White Paper observed that the application scale and level of industrialization in China's IoT market made large-scale adoption and application of IoT devices difficult. The White Paper noted that many industrial products were insufficiently reliable, or were aspirational in nature (i.e., they existed, but could only be implemented in a laboratory environment). In addition, companies entering the IoT product space were still in the beginning stages of their product development, with goods that offered only limited functionality at high costs. The White Paper specifically criticized China's high-end sensor industry for being very inefficient–the sensors it produced were prohibitively expensive and could not be used in large-scale applications.

Third, the 2014 White Paper noted that the many disparate technical requirements for China's IoT industry made it difficult for the state to allocate R&D funding. Because the data collection requirements for individual IoT industries varied wildly, the possibility of researching a singular "breakthrough" technology for IoT development was negated.

Subsequent planning documents for IoT development highlighted many of the same challenges outlined in the 2014 White Paper. A 2015 IoT White Paper by the China Academy of Information and Communications Technology (formerly known as the China Academy of Telecommunications Research) also identified the issues of supply chain decentralization, inadequate scalability, and the diversity of data requirements as three areas in which China's IoT industry must improve. The paper also derided the fragmented nature of China's IoT ecosystem compared to the West, noting that Google, IBM, Cisco, and Intel all promote "vertical integration and horizontal expansion" through the development of core capabilities and strategic alliances, thus enabling them to influence the global IoT ecosystem.[132] The 2015 White Paper specifically highlighted the continuing competitive weakness of China's sensor industry, noting its ongoing technological weakness in basic and smaller IoT sensors, and that no domestic companies were among the twenty organizations with the greatest number of sensor patents filed in China.[133] The 2015 White Paper

[129] "物联网白皮书" (Internet of Things White Paper), 工业和信息化部电信研究院 (China Academy of Telecommunication Research of MIIT), 2014.

[130] Miao Wei 苗圩, "推进物联网产业快速有序发展" (Advance the Quick and Orderly Development of the IoT Industry), *Seeking Truth* 求是, no. 16 (2011), August 15, 2011, http://www.qstheory.cn/zxdk/2011/201116/201108/t20110815_102155.htm; "多项底层技术发力 中国物联网大规模商用迎来窗口期" (Multiple Low-Level Technologies Show Strength, and China's Internet of Things Welcomes the Arrival of a Large-Scale Commercial Window of Opportunity), People's Daily Online 人民网, April 20, 2017, http://finance.people.com.cn/n1/2017/0420/c1004-29223236.html.

[131] (Internet of Things White Paper), (China Academy of Telecommunication Research of MIIT) 2014.

[132]物联网白皮书 (2015 年) (Internet of Things White Paper 2015), 中国信息通信研究院 (China Academy of Information and Communications Technology).

[133] (Internet of Things White Paper 2015), (China Academy of Information and Communications Technology).

also claimed that the standards governing IoT devices were inadequately coordinated, which hindered efforts to regulate the industry as a whole.[134]

CAICT's 2016 IoT White Paper continued to emphasize the same challenges identified in the 2015 version,[135] while identifying two new potential areas of improvement. First, it identified the rise of edge computing, or the deployment of cloud computing resources closer to IoT sensors, as an opportunity for China's IoT manufacturers to dramatically improve the efficiency of IoT data transmission.[136] Second, and most critically, the White Paper noted the need to improve device security for IoT products. CAICT argued that most conventional security measures could not be applied to IoT products, rendering China's IoT infrastructure relatively fragile. To rectify this, CAICT recommended undertaking a comprehensive approach to secure China's IoT infrastructure.[137] The authors specifically referenced the U.S. Department of Homeland Security's "Strategic Principles for Securing the Internet of Things" as a potential model that China could use to secure its own IoT ecosystem.[138]

The most recent analyses of China's IoT development have continued to highlight these key challenges, suggesting that they remain unresolved, or at least require continual refinement. A 2017 IoT White Paper produced by the China Electronic Standardization Institute (中国电子技术标准化研究院) focused on standards development, data sharing, IoT data integration, data gathering, and security as areas that China's IoT industry still needed to improve.[139] It is worth noting that while Chinese government and industry experts have targeted bottlenecks in IoT technology development, they have not tried to steer China towards limited specialization or a particular segment of the IoT industrial ecosystem. There is so much expected new market space in IoT over the next ten years that China has not yet found incentives to concede sources of growth in IoT to other countries or companies.[140]

Chinese analysts have also argued that broader adoption of IoT in a number of industries is still hindered by issues of development and deployment costs, as well as concerns about the reliability and maturity of the technologies. Chinese industry leaders are trying to ensure that the cost to produce and connect IoT-enabled devices is driven lower, since success in developing the IoT market is contingent on spurring participation in as many application areas as possible, so that IoT

[134] (Internet of Things White Paper 2015), (China Academy of Information and Communications Technology).

[135] 2016-物联网白皮书 (2016 年) (Internet of Things White Paper 2016), 中国信息通信研究院 (China Academy of Information and Communications Technology).

[136] The authors highlight the Edge Computing Industry Alliance, a joint initiative undertaken by Huawei, the Shenyang Institute of Automation, Chinese Academy of Sciences, China Institute of Information and Communications, Intel Corporation, ARM, and iSoftStone Information Technology (Group) Co., Ltd. as being a vector by which IoT edge computing can be improved.

[137] 2016-物联网白皮书 (2016 年) (Internet of Things White Paper 2016), 中国信息通信研究院 (China Academy of Information and Communications Technology).

[138] 2016-物联网白皮书 (2016 年) (Internet of Things White Paper 2016), 中国信息通信研究院 (China Academy of Information and Communications Technology).

[139] "工业物联网白皮书" [Industrial Internet of Things White Paper], 中国电子技术标准化研究院 China Electronic Standardization Institute, September 13, 2017, www.cesi.cn/images/editor/20170913/20170913114540317.pdf.

[140] Zhou Ming 周明, "迎接物联网, 拥抱大连接时代" (Greeting the Internet of Things, Embracing the Era of Big Connection), *Huatai Securities 华泰证券*, August 25, 2017, 8-9.

diffusion and adoption can reach its full potential.[141] As Li Yue, China Mobile's president and CEO, recently stated,

> We aim to lower the bar of entry for different vertical industries to enter the IoT ecosystem to the point where module prevalence will remove the bar altogether; for example, if it costs around $5 to connect a refrigerator to the Internet, refrigerator manufacturers will be happy to do so. Thus, we hope that our efforts in terminals will help lower the cost of smart homes, Internet of Vehicles (IoV / 车联网), and wearables, and increase the number of connected devices exponentially.[142]

To address the development needs of the IoT industry, China's government has proposed and enacted policy solutions that include:[143]

- Developing "special action plans" to promote technologies that can drive innovation in specific IoT applications, deepen understanding of network applications, and promote a model of "healthy sustainable development" for the Internet of Things;
- Optimizing and improving funding allocations, with a focus on "the enterprise" (i.e., individual firms) as the main driver of innovation, as well as "strengthening upstream and downstream multi-party cooperation in the industry chain";
- Utilizing IoT technologies to augment traditional industries, developing scalable technologies that can be applied across the IoT industry;
- Carrying out basic R&D of "core technologies and key products" and promoting the development of "indigenously controlled" hardware and software that can be integrated into IoT industry infrastructure;
- Promoting the development of an IoT standards system; and
- Strengthening data processing and comprehensive application development.

Implications for the United States

Chinese policies toward the IoT industry need to be understood in the context of their national strategic imperatives to promote innovation-driven growth and become a global technology leader. The competitive lens through which the Chinese leadership views technology development belies their rhetoric about "win-win cooperation" and their promise that "China will never pursue development at the expense of others' interests."[144] On the contrary, China sees technology development as a decisive strategic resource, and considers other countries' ostensible control of key and core technologies to be a significant strategic liability. China's determination to lead in IoT and 5G development is grounded in these considerations as well as a high sensitivity to the cost of ceding dominance in next-generation technologies to other powers.

[141] "Verticals" is an industry term referring to IoT application areas, which each sustain their own industry ecosystem of devices, software, and product supply chains.

[142] Li Yue 李跃, "China Mobile aims for 1.75 billion connections by 2020," *WinWin*, No. 27 (2017), 13-16, accessed May 17, 2018, http://www-file.huawei.com/-/media/CORPORATE/PDF/publications/winwin/27/win-win-27-en.pdf.

[143] 物联网白皮书 (Internet of Things White Paper), 工业和信息化部电信研究院 (China Academy of Telecommunication Research of MIIT) 2014.

[144] Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," Xinhua Net, November 3, 2017, http://www.xinhuanet.com/english/download/Xi_Jinping%27s_report_at_19th_CPC_National_Congress.pdf.

As a result, Chinese competition in IoT risks becoming a significant challenge for the U.S. in the near future. For now, China's large market size, production capacity, and government support offer it some significant advantages, but it is still behind leading international levels in many IoT technologies. Therefore, U.S. companies and the U.S. government still have time to maintain a technological edge and influence future IoT development, standards, and roll-out. In order to take advantage of this time U.S. actors need to act with urgency and purpose. It is most useful for them to recognize that China views its pursuit of a leading position in the industry as a high stakes competition with direct national security relevance. As such, China's commitment to gaining the upper hand against U.S. competitors will likely be very high, and chances for amicable accommodation are low. It is difficult to forecast the development trajectory of the global IoT marketplace in aggregate given uneven adoption and development rates,[145] but competition from Chinese companies is likely to stiffen. Among other effects, this increased competition will begin to close the window of opportunity for U.S. companies and the U.S. government to enact policies, develop standards, and deploy products that can ensure that future IoT development continues on favorable terms for U.S. consumers and corporate entities.

China's IoT policies share commonalities with the Chinese development approach to other high technology industries, starting with a prioritization of "top-level design" (顶层设计) as the key to marshalling national resources towards a strategic goal. Through its multiple planning documents, the Chinese government seeks to guide development activities, acting as an indispensable catalyst for faster development in areas that best promote national interests. This strategic planning is consciously grounded in market-based economic logic, but the government's top-down, holistic drive towards development of key industries inevitably distorts normal market behavior. As a result, major Chinese corporations in strategic industries face a difficult, if not impossible challenge to avoid being affected by the Chinese government's policy priorities. U.S. corporations competing with Chinese firms in these industries must be aware that they are considered strategic rivals by the Chinese government, if not outright threats, and that even private-sector competition will be met with a zero-sum approach. This approach is ultimately detrimental to U.S. national security and economic interests in both the immediate and long term.

Given these considerations, it is not clear if U.S. IoT firms will be welcome to participate in China's IoT development on beneficial or even fair terms. China's practice of economic protectionism in specific economic sectors is likely to extend to some important IoT applications, and its approach towards information and network security as matters of national security are likely to hamstring U.S. IoT firms from participating fully or fairly in China's burgeoning IoT market. These specific roadblocks that directly result from China's IoT strategy are covered in detail below.

Restrictions on Foreign Investment

By some measures the Chinese economy is extremely open to investment from foreign IoT firms. The 2017 Catalogue for Guidance of Foreign Investment Industries (外商投资产业指导目录) issued by the NDRC includes "development and application of Internet of Things technology" as

[145] For instance, smartwatches are considered a fairly mature market with a wide consumer base, while IoT-enabled automobiles are not projected to be made widely available until 2040. See "Smartwatch Market Overview," Prescient and Strategic Market Research, February 2018, https://www.psmarketresearch.com/market-analysis/smartwatch-market and Gene Munster and Austin Bohlig, "Auto Outlook 2040: The Rise of Fully Autonomous Vehicles," Loup Ventures, September 6, 2017, https://loupventures.com/auto-outlook-2040-the-rise-of-fully-autonomous-vehicles/.

a service sector in which foreign investment is encouraged.[146] Additionally, hardware components that could be used in IoT devices such as automobile electronics, computer components, sensors, and audio-visual equipment are also listed as "encouraged industries for foreign investment."[147] Chinese state-planners appear eager to leverage foreign know-how and investment in China's adoption of the IoT.

Other indications, however, suggest that foreign participation in China's IoT market will be severely restricted. The same Catalogue for Guidance of Foreign Investment Industries that identified IoT technology and relevant subcomponents as encouraged areas for foreign investment also marks 35 economic sectors as "restricted" and subject to increased regulation.[148] These sectors include areas that represent major market opportunities for IoT firms, including shipping, satellites, power grids, railroads, aerospace, oil and gas, health care, and telecommunications.[149] In order to gain market access to these sectors, foreign firms must undergo a lengthy approval process that is not required of their local counterparts.[150] Foreign firms also may be required to enter into a joint venture with a Chinese partner and comply with local equity requirements.[151] These restrictions on lucrative sectors for foreign IoT companies may limit foreign competitiveness in the Chinese market.

Selective Enforcement of Chinese Laws in Favor of Domestic Companies

The specter of Chinese government regulation has real-world consequences for U.S. IoT firms, much as it has already impacted U.S. firms operating in other industries in China. Although Chinese regulations governing foreign investment are ostensibly not dissimilar from those of other large economies, in practice they are often selectively enforced in a way which penalizes foreign companies. All IoT firms operating within China are required to comply with a variety of Chinese laws. In practice, however, these laws and regulations have been used as a cudgel to harass or impede the development of foreign firms operating within China, but not their domestic Chinese competitors. Some examples include:

[146] "外商投资产业指导目录 (2017 年修订)" (Catalogue of Industries for Guiding Foreign Investment (Revision 2017)), National Development and Reform Commission and the Ministry of Commerce of the People's Republic of China, accessed June 17, 2018, http://www.ndrc.gov.cn/zcfb/zcfbl/201706/W020170628553266458339.pdf.

[147] (Catalogue of Industries for Guiding Foreign Investment (Revision 2017)), National Development and Reform Commission and the Ministry of Commerce of the People's Republic of China.

[148] "外商投资产业指导目录 (2017 年修订)" (Catalogue of Industries for Guiding Foreign Investment (Revision 2017)), 中华人民共和国国家发展和改革委员会 (National Development and Reform Commission of the People's Republic of China) and 中华人民共和国商务部 (Ministry of Commerce of the People's Republic of China), accessed June 17, 2018, http://www.ndrc.gov.cn/zcfb/zcfbl/201706/W020170628553266458339.pdf.

[149] "外商投资产业指导目录 (2017 年修订)" (Catalogue of Industries for Guiding Foreign Investment (Revision 2017)), National Development and Reform Commission and the Ministry of Commerce of the People's Republic of China, accessed June 17, 2018, http://www.ndrc.gov.cn/zcfb/zcfbl/201706/W020170628553266458339.pdf.

[150] "Competition Policy and Enforcement in China," US-China Business Council, accessed July 18, 2018, https://www.uschina.org/sites/default/files/AML%202014%20Report%20FINAL_0.pdf.

[151] 中华人民共和国中外合资经营企业法实施条例 (Regulations for the Implementation of the Law on Sino-Foreign Equity Joint Ventures), Ministry of Commerce of the People's Republic of China, December 26, 2017, http://www.mofcom.gov.cn/article/zt_swfg/subjectby/200612/20061204134636.shtml; "Measures and Practices Restraining Foreign Investment in China," Covington & Burling LLP, accessed July 18, 2018, http://trade.ec.europa.eu/doclib/docs/2014/august/tradoc_152739.08.10.pdf.

- "*Measures for the Protection of Information Security Levels" (信息安全等级保护管理办法), also referred to as the "Multi-Level Protection Scheme" (MLPS):* The MLPS outlines five security levels that can be applied to information and data management systems, but their ambiguous wording leaves them open to wide and possibly unfair interpretation by the Chinese government.[152] Damage to "level 1" systems would harm the legal rights of citizens within China, while damage to "level 5" systems would result in "very serious harm" to the national security of the PRC.[153] Under current MLPS standards, any IoT device that monitors or collects customer data would be subject to regulation. While all IoT firms in China must abide by the MLPS, its provisions are frequently criticized for placing unnecessary and cumbersome burdens on foreign firms seeking to operate within China. The MLPS places restrictions on which hardware and software components can be used in products that process sensitive data,[154] a stipulation that critics have argued "[suggests] an outright discriminatory preference for domestic IT solutions."[155] Under the MLPS, certain products which collect user data are required to use Chinese intellectual property for key hardware components and must be certified by the China Compulsory Certification (CCC) for information security products.[156] According to U.S.-China Business Council (USCBC) interviews, the hardware and software requirements mandated by the MLPS are unevenly enforced and are sometimes ignored altogether.[157] Given the emphasis placed on domestic production in strategic planning initiatives related to the IoT, the government has incentives to enforce these rules even more stringently in the future.
- *Laws protecting "critical information infrastructure":* The IoT's status as an IT sector and its close relationship to the telecommunications sector means that IoT firms are also subject to China's draconian and vaguely worded Cybersecurity Law (网络安全法) and other legal provisions that nominally entitle the Chinese government to protect "critical information infrastructure (关键信息基础设施)," which likely covers IoT devices and providers.[158] The Cybersecurity Law also states that "critical information infrastructure providers" must store their data within China, under the jurisdiction of the PRC.[159] Since the term "critical information infrastructure provider" is extremely vague, it is plausible that this law could be applied to designers, manufacturers, and distributors of IoT devices. China has not clarified whether this is the case. Other documents, like the National Network Security Inspection Operational Guidance (国家网络安全检查操作指南), stipulate that energy, transportation, and industrial manufacturing with potential IoT applications are subject to

[152] "信息安全等级保护管理办法" [Measures for the Protection of Information Security Levels], Ministry of Public Security, July 24, 2007, http://www.gov.cn/gzdt/2007-07/24/content_694380.htm.

[153] [Measures for the Protection of Information Security Levels], Ministry of Public Security.

[154] [Measures for the Protection of Information Security Levels], Ministry of Public Security.

[155] Nick Marro, "The Five Levels of Information Security in China," *China Business Review*, December 5, 2016, accessed July 22, 2018, https://www.chinabusinessreview.com/the-5-levels-of-information-security-in-china/.

[156] Marro, "The Five Levels of Information Security in China."

[157] Marro, "The Five Levels of Information Security in China."

[158] "中华人民共和国国家安全法" (National Cybersecurity Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed July 18, 2018, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

[159] (National Cybersecurity Law of the People's Republic of China).

inspection, specifically mentioning industrial IoT as critical information infrastructure deserving of regulation.[160]

- *Anti-Monopoly Law (反垄断法):* China's 2007 Anti-Monopoly Law grants considerable regulatory authorities to China's State Administration for Industry and Commerce (SAIC) and the NDRC to target and investigate entities within China suspected of violating anti-trust laws.[161] A 2014 U.S. China Business Council survey found that 86 percent of its member firms were either "somewhat or very concerned" about being targeted by the Chinese government under existing anti-trust laws within China.[162] Some of these investigations are perceived as tools to penalize foreign companies in favor of China's domestic firms.[163]

The Prospect of Technology Transfer

In addition to legal and policy challenges, U.S. firms are frequently forced to navigate unofficial requirements from their Chinese counterparts and government regulators that may include technology transfer. Since its entry in 2001, China has technically complied with WTO regulations which prohibit member states from undertaking certain coercive trade practices, such as legally mandating that foreign entities transfer technology to their local counterparts.[164] Additionally, CCP officials have been extremely vocal in claiming that the PRC does not legally require foreign firms to transfer technology.[165] Nevertheless, China often levies numerous indirect requirements on foreign entities, especially ones operating in fields that Beijing deems strategically vital.[166]

The IoT is one such strategically important field that is potentially a target for technology transfer. While complete statistics are not always forthcoming, of the U.S. companies operating in China surveyed in 2017 by the USCBC, nearly one fifth reported being requested to undertake some form

[160] "国家网络安全检查操作指南" (National Network Security Inspection Operational Guidance), CCP Central Committee Office of the Leading Small Group for Internet Security and Informatization, June 2016, http://wlzx.hebtu.edu.cn/resources/43/20161027101045853.doc

[161] "中华人民共和国反垄断法" (Anti-Monopoly Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed July 18, 2018, http://www.gov.cn/flfg/2007-08/30/content_732591.htm; "Competition Policy and Enforcement in China," U.S.-China Business Council, accessed July 18, 2018, https://www.uschina.org/sites/default/files/AML%202014%20Report%20FINAL_0.pdf.

[162] "Competition Policy and Enforcement in China," U.S.-China Business Council, accessed July 18, 2018, https://www.uschina.org/sites/default/files/AML%202014%20Report%20FINAL_0.pdf.

[163] Rich McCormick, "Qualcomm Fined $975 Million by Chinese Anti-Monopoly Regulators," *The Verge,* February 9, 2015, https://www.theverge.com/2015/2/9/8009589/qualcomm-fined-975-million-by-chinese-anti-monopoly-regulators.

[164] Although China claims to be in compliance with existing WTO regulations on technology transfer, as of May 2018 it is currently being litigated for alleged violations of international trade law; Tom Miles, "U.S. and China Clash over 'Technology Transfer' at WTO," Reuters, May 28, 2018, https://www.reuters.com/article/us-usa-trade-china/u-s-and-china-clash-over-technology-transfer-at-wto-idUSKCN1IT11G.

[165] According to the USTR, these claims have been made almost every year for the past decade through outlets such as the U.S.–China Strategic and Economic Dialogue and the U.S.-China Joint Commission on Commerce and Trade, as well as through Xi Jinping's official statements; "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," Office of the United States Trade Representative Executive Office of the President, accessed July 14, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[166] "Findings of the Investigation into China's Acts, Policies, and Practices," Office of the United States Trade Representative Executive Office of the President.

of technology transfer.[167] These requests are often poorly documented, and are not part of contractual agreements between U.S. and Chinese firms. However, an inquiry by the USTR found that PRC officials relied on "oral communications and informal 'administrative guidance' to pressure foreign firms to transfer technology."[168] Substantial anecdotal evidence suggests that failure to comply with these requests can result in firms being denied key licenses, as well as harassment by Chinese regulatory authorities, or disbarment from the Chinese market altogether.[169] Although no formal study has been conducted examining how IoT firms are specifically impacted by these coercive trade practices, it is likely that they would be subject to similar demands for similar concessions.

In the aggregate, it is clear that China's restrictions governing foreign investment are far more extensive than those employed by other developed nations. Moreover, it is clear that these policies are being enacted in order for Chinese firms to gain competitive edge over their foreign counterparts. This has significant implications for the state of the global IoT industry. In the short term, it is likely that U.S. IoT firms will face demands to engage in technology transfer as a prerequisite to entering the Chinese marketplace. Acquiescence to these demands will likely erode technological advantages held by U.S. IoT companies operating within China, and will better position Chinese IoT firms to compete in the global marketplace. In the longer term, it is likely that profits for U.S. firms operating in China will diminish as China's IoT industry continues to mature with governmental support. This could lead to U.S. IoT firms voluntarily exiting China's marketplace altogether.

Recommendations

While there may be little policy recourse to effectively counter China's state-driven IoT development, some of the effects of China's IoT strategy may be mitigated. However, any effort to level the playing field for U.S. IoT firms operating within China must come as part of a broader effort to remedy some of the existing problems in the U.S.-China trade relationship. Hence, while the following recommendations are specific to IoT firms operating within China, they can also be applied to bolster the position of all U.S. firms operating within that market space.

1. Commission a blue-ribbon panel with a mandate to assess the ability of the United States to compete in emerging commercial information and communications technologies.

Given the transformative potential of the IoT and other emerging technologies, the United States should convene experts at the highest level to evaluate the current state of U.S. technological development and discuss ways to ensure U.S. competitiveness in the new generation of information and communications technologies.

[167] "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974," Office of the United States Trade Representative Executive Office of the President, accessed July 14, 2018, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

[168] "Findings of the Investigation into China's Acts, Policies, and Practices," Office of the United States Trade Representative Executive Office of the President.

[169] "Findings of the Investigation into China's Acts, Policies, and Practices," Office of the United States Trade Representative Executive Office of the President.

2. Publish a list of federal guidelines laying out "best practices" for IoT firms seeking to operate within China.

A number of sources within the Western legal and business community have documented the challenges faced by firms seeking to operate within China.[170] However, there is currently no unified, authoritative guide to conducting business in China. Therefore, the federal government should promulgate an official set of guidelines advising IoT firms on how to navigate the Chinese marketplace. While some of these services are already provided by the U.S. Commercial Service (the trade promotion arm of the U.S. Department of Commerce's International Trade Administration), a streamlined, widely-distributed primer with advice on best practices for entering into joint ventures with local firms, avoiding forced technology transfer, and protecting IP would better protect U.S. companies and raise awareness.

3. Continue to seek legal redress against coercive Chinese trade practices through international institutions.

The United States should work through existing international trade institutions to hold China accountable for unfair trade practices. Some initial steps towards this end have already been made. For example, in August 2017, the USTR invoked Section 301 of the 1974 Trade Act in response to alleged IP theft from China, and in March 2018 brought a WTO case against Chinese licensing regulations.[171] A continued effort should be made to publicly highlight cases of unfair trade practices occurring, as well as seeking means of legal redress through organizations like the WTO.

4. Collaborate with partner nations to counter coercive Chinese trade practices

Many of the challenges faced by U.S. IoT firms operating within China are shared by other foreign firms.[172] Therefore, U.S. legal and economic efforts to counter China's unfair trade practices should be coordinated with partners in Europe and East Asia. The United States should also seek to expand existing trade partnerships in the Asia-Pacific region to build a larger shared market that could act as a counterweight to China's economic power.

[170] Dan Harris, "China Joint Ventures: Keeping Your Friends Close and Your IP Closer," China Law Blog, *Harris Bricken*, April 6, 2018, https://www.chinalawblog.com/2018/04/china-joint-ventures-keeping-your-friends-close-and-your-ip-closer.html.

[171] "USTR Announces Initiation of Section 301 Investigation of China," Office of the United States Trade Representative, August 2017, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2017/august/ustr-announces-initiation-section; "Following President Trump's Section 301 Decisions, USTR Launches New WTO Challenge Against China," March 2018, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/march/following-president-trump%E2%80%99s-section.

[172] Jonathan Stearns, "EU Takes China to the WTO over Technology-Transfer Practices," *Bloomberg*, June 1, 2018, https://www.bloomberg.com/news/articles/2018-06-01/europe-takes-china-to-the-wto-over-technology-transfer-practices.

Chapter 2: The Standards Race

While the international standards system has in the past favored market leaders, allowing new standards to emerge through a voluntary system based on the ad-hoc participation of experts and companies, China is upsetting this status quo. By leveraging a coordinated standards-setting strategy that involves efforts both at home and abroad, Beijing is bringing increasing pressure to bear on an international standardization system not designed to withstand a concerted effort at manipulation. The country's increased participation combined with its market share has already shifted the power balance in key standards venues like the Third Generation Partnership Project (3GPP) in China's favor.[173] At the same time, China is pushing to change the primary fora for these negotiations to standards-setting organizations in which it can more easily dominate.

China's interest in influencing international standards stems from the recognition of the economic, political, and security advantages conferred upon the nations that set technology standards. In this sense, China's "standardization work" (标准化工作) is as much about national rejuvenation as it is a legacy of Communist-inspired central economic planning and has matured into an important part of a techno-nationalist development strategy. Elevating a homegrown technology to serve as the international standard yields a tremendous commercial advantage, which can then be leveraged to gain even more market share and dominance over particular industries. This advantage is magnified from a security viewpoint, as the originator of a standard technology has an intimate understanding of how it operates inside and out.

For these reasons, standards have become an important part of China's grand strategy featuring high-level bureaucratic coordination, significant state financial support, and a fusion of state resources and free-market dynamism. The government actively encourages domestic technology standardization that consolidates China's considerable domestic market power around standards that Beijing finds acceptable with a strong emphasis on controlling and accelerating Chinese development of the IoT and 5G. This whole-of-country strategy has allowed China to develop, standardize, and promote its standards abroad, facilitating the widespread adoption of its homegrown technologies.

China's expansion of its techno-nationalist standardization efforts takes on a special importance given the fragmented and nascent state of IoT standardization around the world. Existing IoT and 5G standards are part of a nascent, fragmented and complex standards-setting environment rife with incompatible proprietary solutions and a veritable alphabet soup of standards-setting bodies. China's concerted efforts to export its preferred standards to the international stage are likely to have an outsize impact on global IoT standards in such a fragmented standards-setting environment and at a critical juncture while many pivotal technologies are coming into widespread use.

Internationally, China has adopted a two-pronged approach to ensure the adoption of Chinese standards. It uses its growing market influence and increased representation in international standards bodies to shape standards from the top-down while pushing to ensure widespread adoption of its technologies from the bottom up, both at home and through infrastructure contracts with developing countries. This is accomplished largely under the auspices of the One Belt, One Road strategy (also known as the Belt and Road Initiative, or BRI), and serves to make Chinese

[173] Dave Burstein, "China: We Lead 3GPP Wireless Standards," *CircleID*, May 26, 2018, http://www.circleid.com/posts/20180526_china_we_lead_3gpp_wireless_standards/.

technologies the *de facto* standard in large parts of the world.[174] These two tactics are mutually reinforcing: the ability to demonstrate widespread adoption lends Chinese standards weight in international standards consideration, while the approval of Chinese technical standards on the global level increases their marketability.

Inside international standards organizations, China has dramatically increased its influence in recent decades. It is investing heavily in pivotal standards bodies and in sending large delegations to attend meetings where Chinese firms submit so many contributions that they have been accused of "flooding the process." Chinese representatives are widespread in working and technical committees across international standards organizations, and Chinese experts are assuming key leadership roles in global standards organizations while continuing to espouse nationalistic rhetoric and promoting Chinese national standards-setting efforts before and after their tenures. Above all, China coordinates lobbying efforts and pressures its companies in critical standards votes to ensure the adoption of homegrown tech standards.

China understands that a large part of standards influence comes from ubiquity. For this reason, it prioritizes and invests in R&D that will allow it to gain first-mover advantage stemming from technological leadership. China pursues this practical advantage in tandem with efforts to draft official standards, knowing that a demonstrable prevalence of products using its standards will help persuade international organizations to accept them. This strategy is clearly demonstrated in the state-driven development of 5G technologies that Chinese national champion companies are racing to unveil. China also offers state backing to companies to establish themselves worldwide and artificially inflates its market advantage by baking acceptance of its technical standards into foreign policies like the BRI. In offering other countries deals on its technologies and converting them to use Chinese standards, China also helps secure their support at international standards bodies. At home, China leverages its market size to win compliance with its preferred technical standards even in the absence of their official adoption, allowing Chinese companies to escape paying royalties to foreign intellectual property rights (IPR) holders and ensuring that the products sold in China conform to the state's defined "national security" specifications. With regard to telecommunications technologies, this regulatory strategy has implications for free access to the internet for Chinese citizens and citizens of any other nation where such products are sold.

Already, this strategy is yielding success: China is winning key standards votes that will help to entrench its companies in the market for critical technology ecosystems like the IoT and catalytic technologies like 5G at a pivotal time when the international community is working to lay the foundation for the next generation of technological development. China's wins are evident in early standards for 5G that have already been finalized, and it is working to be among the first countries to debut a widespread 5G network, which would strengthen its position in negotiations still to come in 2019.

This chapter documents Chinese efforts to set international standards for the IoT and evaluates the economic and national security implications for the United States. The first section provides an overview of the current standards landscape for IoT products and related enabling technologies like 5G. The second section briefly describes the U.S. standardization efforts in international standards bodies as a key component of the current overall standards landscape. The third section analyzes China's state-driven *modus operandi* for implementing technical standardization for the

[174] Polk, "China is Quietly Setting Global Standards."

IoT, covering its strategic significance and domestic and international standardization efforts. The fourth section explores key points of contention between the United States and China, highlighting critical areas of focus for U.S. policymakers. This chapter concludes with an assessment of ongoing IoT standardization efforts in the United States, China, and the international sphere and includes recommended steps for the United States to maximize the benefits of the ongoing standardization.

Setting IoT Standards

Existing international IoT standards are piecemeal and key areas are still up for debate, creating opportunities for companies and nations investing in innovation to assert themselves in shaping standards and reap the benefits that come with owning standard-essential technology. The challenge comes in the standards-setting environment, which for the IoT and enabling technologies like 5G is especially fragmented, complex, and populated by an overabundance of prospective standards and standards-setting bodies.[175]

Standards take on tremendous economic significance because companies (and the home countries that rely on them as engines of growth) benefit when their innovative technology is adopted as a global standard. This allows them to sell their products more broadly or earn royalties from licensing their standards-compliant patents to manufacturers that develop devices under that standard and other downstream companies.[176] Favorable positioning in a new technology can be pivotal for companies: for example, when 4G technology was released (for which Qualcomm held an estimated 21 percent of the patents),[177] the company recorded seven consecutive quarters of 25 percent-plus growth.[178] 5G is also expected to add significant profit for Qualcomm, and it has been cited as a growth factor in revising the company's profit forecast upward.[179] The company garnered attention for announcing plans to charge royalties on its 5G NR standard patents as a percentage of the sale price of 5G smartphones, up to $16.25 per phone.[180] Conversely, when other companies own key standard components, downstream companies must either buy or license that technology. As standards-takers rather than standards-makers, Chinese companies have been left out of the royalty game in the past while U.S. companies have benefitted from the use of U.S. standards around the world.[181]

Beyond national or corporate advantage, standards ensure functionality and interoperability across these varied devices and platforms worldwide, and in turn support the field's general profitability,

[175] Dave Burstein, "China: We Lead 3GPP Wireless Standards," *CircleID*, May 26, 2018, http://www.circleid.com/posts/20180526_china_we_lead_3gpp_wireless_standards/. blog/IoT-Agenda/A-world-with-more-IoT-standards-bodies-than-IoT-standards.

[176] Andrew Polk, "China is Quietly Setting Global Standards," *Bloomberg*, May 6, 2018. https://www.bloomberg.com/view/articles/2018-05-06/china-is-quietly-setting-global-standards.

[177] Bill Ray, "Who owns 4G mobile technology?," *The Register,* September 23, 2011, https://www.theregister.co.uk/2011/09/23/lte_patent_pie/.

[178] Jonathan Cooper, "Qualcomm: The Sky Is the Limit as 5G Approaches," *Seeking Alpha*, September 26, 2018, https://seekingalpha.com/article/4208339-qualcomm-sky-limit-5g-approaches.

[179] Dan Jones, "Qualcomm Raises Profit Forecast for FY19, Citing 5G & More," January 18, 2018, *Light Reading*, https://www.lightreading.com/components/mobile-wireless-components/qualcomm-raises-profit-forecast-for-fy19-citing-5g-and-more/d/d-id/739777.

[180] Mike Dano, "Qualcomm to Charge Up to $16.25 in Royalties for Every 5G phone, More Than Ericsson's $5/Phone," November 28, 2017, *Fierce Wireless,* https://www.fiercewireless.com/5g/qualcomm-to-charge-up-to-16-25-royalties-for-every-5g-phone-more-than-ericsson-s-5-phone.

[181] Polk, "China is Quietly Setting Global Standards."

technological development and innovation, and privacy and security measures. Absent a unified standards regime, experts predict that IoT as a field will progress more slowly, be more expensive, and result in lower quality and increased risk.[182] Going without standardization means accepting unknown risk, which in addition to operational, security, and privacy drawbacks, may run counter to other existing legal and regulatory regimes. The IoT presents greater vulnerability to the cascading impact of compromise when a single device is linked to a network of other devices, creating increased interdependency and a greater need for security.[183]

Industry association-developed standards are often adopted faster than legal mandates forced to move at the slow pace of legislation. More brand-agnostic than vendor-led consortia, industry association standards tend to focus on technical interoperability and product quality, which helps avoid proprietary traps that slow market growth, although they also have a history of overlooking the public interest when it conflicts with their goals.[184] Industry-formulated standards rarely become national law, though most major companies are involved in domestic lobbying and intergovernmental regulatory efforts to advance their interests. Some IoT experts believe that "technology vendors play perhaps too prominent a role" in most of the many IoT standards bodies.[185]

Beyond its capacity to offer directives that are legally binding, government regulation is needed to fill gaps that industry self-regulation efforts cannot or will not address.[186] Security is one such area where a market failure is likely to occur, as unsecured devices from security cameras to appliances can still function without sufficient investments in security. The absence of market incentive for companies to build in security features such as updates for firmware leads to the current levels of system-wide security vulnerability.[187] For these reasons, this chapter will focus more on national government and international standards over industry-derived groups and their proposed standards.

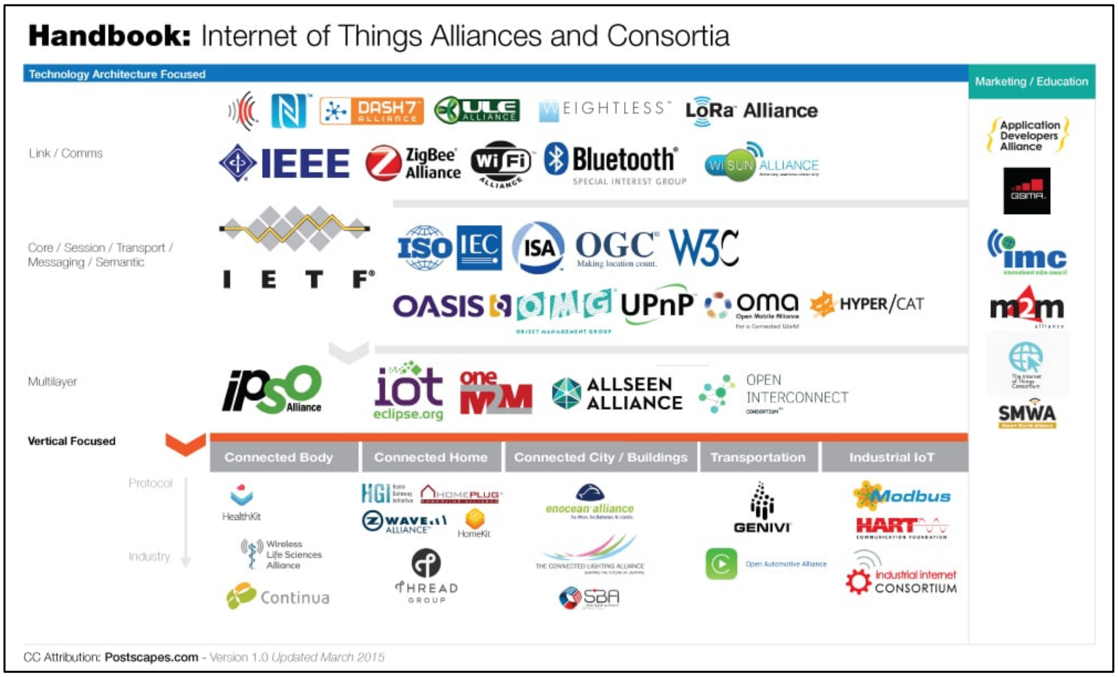
A Fractured Standards-Setting Environment

Within the standards landscape are two types of IoT (industrial and consumer), three types of standards (management/business, operational, and technical), four technological layers (application, service, network, and access technology), and many entities drafting standards and specifications.[188] These entities range from organizations pushing open source software to define

[182] Tyson Macaulay, *RIoT Control: Understanding and Managing Risks and the Internet of Things* (New York: Morgan Kaufmann, 2017).
[183] Macaulay, *RIoT Control*.
[184] Macaulay, *RIoT Control*.
[185] Thomas H. Davenport and Sanjay E. Sarma, "Setting Standards for the Internet of Things," *Harvard Business Review*, November 21, 2014, https://hbr.org/2014/11/setting-standards-for-the-internet-of-things; Bruce Sinclair, "A Symbiotic Partnership between Standards Bodies and Consortia," panel discussion with Carsten Bormann, Amine Chigani, Michael Koster, and Michael Richardson, *The IoT Inc Business Show*, podcast audio, episode 11, March 17, 2018, https://www.iot-inc.com/internet-of-things-standards-bodies-consortia-podcast/.
[186] Macaulay, *RIoT Control*.
[187] Oscar Williams-Grut, "Hackers Once Stole a Casino's High-Roller Database Through a Thermometer in the Lobby Fish Tank," *Business Insider*, April 15, 2018, http://www.businessinsider.de/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=UK&IR=T.
[188] An exact number of drafting entities is difficult to estimate given the many different types of standards-setting efforts, the many applications of the IoT, and the variety of corporate, government, and international bodies and various sub-committees involved. There are more than 50 such organizations in existence.

a de facto standard (e.g., EdgeX Foundry),[189] to corporate-sponsored vendor alliances highlighting proprietary solutions, to industry associations, to national governing agencies, to intergovernmental bodies. Many of the bodies focused on standardizing the underlying architecture for the IoT are vendor-led groups promoting proprietary solutions that will not be cross-compatible without broader overarching regulation. Given that the IoT spans many industries, different industries also have their own IoT consortia. For an indication of the complexity and stratification of private-sector IoT standards bodies, see Figure 1.[190]

Figure 1: IoT Alliances and Consortia



CC Attribution: Postscapes.com - Version 1.0 Updated March 2015

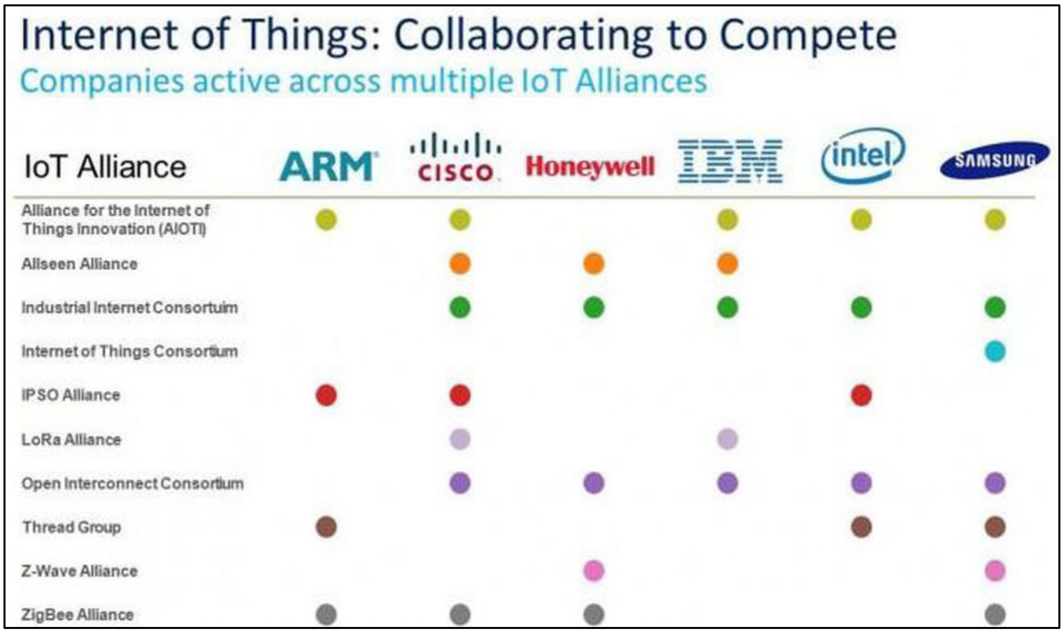
Many of the largest companies such as Cisco and IBM are involved in multiple standard-setting efforts, indicating less a promise to coordinate between them than an attempt to both hedge their bets and influence the direction of such groups (see Figure 2).[191]

[189] Michelle Heathers, "The Complexity of Standards in IoT," *Open Stand*, October 4, 2017, https://open-stand.org/the-complexity-of-standards-in-iot/.

[190] IoT Alliances and Consortium: A Guide to the Range of Alliances and Consortia Targeting Internet of Things Technology Layers and Industry Verticals," Postscapes.com, June 20, 2018, https://www.postscapes.com/internet-of-things-alliances-roundup/.

[191] Stephen Lawson, "Is 2017 the Year IoT Standards Finally Make Sense?" January 13, 2017, *IDG News Service*, https://www.computerworld.com/article/3157421/internet-of-things/is-2017-the-year-iot-standards-finally-make-sense.html; Theo Priestley, "The Internet of Things Is a Fragmented $19 Trillion Roulette Gamble," *Forbes*, October 5, 2015, https://www.forbes.com/sites/theopriestley/2015/10/05/the-internet-of-things-is-a-fragmented-19-trillion-roulette-gamble/#55e30fe929d9.

Figure 2: Major Company Participation in IoT Alliances



Internet of Things: Collaborating to Compete

Companies active across multiple IoT Alliances

IoT Alliance	ARM	CISCO	Honeywell	IBM	intel	SAMSUNG
Alliance for the Internet of Things Innovation (AIOTI)	●	●		●	●	●
Allseen Alliance		●	●	●		
Industrial Internet Consortuim		●	●	●	●	●
Internet of Things Consortium						●
IPSO Alliance	●	●			●	
LoRa Alliance		●		●		
Open Interconnect Consortium		●	●	●	●	●
Thread Group	●				●	●
Z-Wave Alliance			●			●
ZigBee Alliance	●	●	●			●

This challenge is exacerbated by a fracturing of the provider space. The IoT is characterized by a complex web of independently developed IoT devices, systems, and services. Instead of one provider of an integrated suite of services, there are many competing providers for endpoints, gateways, networks, and data centers and cloud services. Without standards, each system would need individual and unique security investments and assessment, and harmonizing different devices, systems, and services would require specific bilateral efforts. The risk is that competing, incompatible standards can dissuade product designers and consumers from committing to a standard. For instance, devices requiring low range and medium-to-low data rate can choose from Bluetooth, LTE Category 0, and ZigBee, making it hard for the market to coalesce around one type of communication conduit.[192] Standardization is particularly important on the application programming interface (API) level to scale for the demands of IoT so that not every provider has to form a multiplicity of relationships with other providers to create interoperability.[193] One programming website notes that there are some 320 APIs available for IoT uses, illustrating the diversity of the ecosystem.[194]

[192] Harald Bauer, Mark Patel, and Jan Veira, "Internet of Things: Opportunities and Challenges for Semiconductor Companies," McKinsey & Company, October 2015, https://www.mckinsey.com/industries/semiconductors/our-insights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies.

[193] Jennifer Riggins, "APIs Are the Backbone of New IoT Standards, *ProgrammableWeb*, May 11, 2017, https://www.programmableweb.com/news/how-apis-are-backbone-new-iot-standards/analysis/2017/05/11?_ke=c2hhbmEucGVhcmxtYW5AbXVsZXNvZnQuY29t; Kelly Hill, "What is an IoT API?" *RCR Wireless News,* October 18, 2016, https://www.rcrwireless.com/20161018/internet-of-things/what-is-an-iot-api-tag6-tag99; Erik Guttman, "3GPP Initiates Common API Framework Study," 3GPP, May 9, 2017, http://www.3gpp.org/news-events/3gpp-news/1854-common_api.

[194] "Category: Internet of Things," *ProgrammableWeb*, accessed September 5, 2018, https://www.programmableweb.com/category/internet-things/api?pw_view_display_id=apis_all&page=1.

Major International Standards Bodies

Leading international standardizations bodies include big-tent multi-stakeholder industry and technical associations like the Internet Engineering Task Force (IETF), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE), while others like the International Standards Organization (ISO) and the Third-Generation Partnership Project (3GPP) operate by bringing national standards-setting bodies together. In the United Nations, the International Telecommunications Union (ITU) plays a leading role in efforts to standardize the IoT through its ITU Telecommunication Standardization Sector division (ITU-T). Within these bodies, there are also differences in size and scope: for example, 3GPP counts only seven telecommunications associations as organizational partners (though it also allows companies to participate through membership in an organizational partner standards body) while the ISO counts 160 national standards bodies in its membership. Likewise, while 3GPP focuses only on mobile technology, the ISO spans many industries, and the IEC focuses on electrotechnology. The main international standards organizations that are shaping IoT standards are briefly described in the table below.

Table 4: Major International Standards Bodies

Organization	Organization Type	Standards Type	Members	IoT-Specific Bodies
International Standardization Organization (ISO)	Independent, non-governmental international organization	Proprietary industrial and commercial standards derived through a consensus-driven process	162 national standards bodies (one member per country)	• Joint technical committee sub-committee on IoT (ISO/IEC JTC 1/SC 41) with IEC[195] • Several other joint technical committees address specific aspects of IoT activity[196]
International Electrotechnical Commission (IEC)	Non-profit, "quasi-governmental" organization[197]	Electrotechnology standards derived through a consensus-based process	Members are national committees (62 full and 24 associate members) that appoint experts and delegates from industry, commerce, government, test and research labs, academia and consumer groups[198]	• ISO/IEC JTC 1/SC 41 (with ISO) and several other joint technical committees on specific aspects of the IoT[199]
Internet Engineering Task Force (IETF)	Open standards organization under the Internet Society,	Voluntary internet standards, specifically Internet Protocol suite (TCP/IP)[200]	Individual volunteers, no formal membership[201]	• Internet of Things Directorate expert advisory group[202]

[195] "ISO/IEC JTC 1/SC 41 Scope," International Electrotechnical Commission (IEC), accessed July 23, 2018, http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:20486.

[196] "SC 41 Business Plan and Dashboard 2017," ISO/IEC JTC 1, N 13538 August 30, 2017, http://www.iec.ch/public/miscfiles/sbp/jtc1-sc41.pdf.

[197] "Who We Are," International Electrotechnical Commission (IEC), accessed September 4, 2018, http://www.iec.ch/about/profile/?ref=menu.

[198] "About the IEC," International Electrotechnical Commission, accessed September 4, 2018, http://www.iec.ch/about/?ref=menu.

[199] "SC 41 Business Plan and Dashboard 2017," ISO/IEC JTC 1, N 13538 August 30, 2017, http://www.iec.ch/public/miscfiles/sbp/jtc1-sc41.pdf.

[200] "Who We Are," Internet Engineering Task Force (IETF), accessed July 23, 2018, https://www.ietf.org/about/who/.

[201] "Mission and Principles," Internet Engineering Task Force (IETF), accessed July 23, 2018, https://www.ietf.org/about/mission/.

[202] "Internet of Things Directorate," Internet Engineering Task Force (IETF), accessed July 23, 2018, https://datatracker.ietf.org/group/iotdir/about/.

	a U.S.-based nonprofit			
Institute of Electrical and Electronics Engineers–Standards Association (IEEE-SA)	Technical professional association	Key communications technology standards	Allows individuals and corporations to become members[203]	• Project 2413 (P2413), founded in 2014 with the aim of producing an overarching architectural framework for the IoT[204]
Third Generation Partnership Project (3GPP)	Collaboration between standards associations	Standards allow entities to claim IPR in the standards-setting bodies that make up the partnership	7 Organizational Partners (regional and national telecoms standards associations)	• Formulates influential 5G standards, which will facilitate more widespread IoT usage, but does not work on IoT-specific standards
International Telecommunications Union, Telecommunication Standardization Sector (ITU-T)	A division of the ITU, a specialized agency of the United Nations	Voluntary, influential recommendations[205]	193 member states,[206] plus 266 sector members and 6 associates[207]	• ITU-T Study Group 20 (SG 20)

[203] "Get Involved with the IEEE-SA," IEEE Standards Association, accessed July 23, 2018, https://standards.ieee.org/getinvolved/index.html.

[204] "Standard for an Architectural Framework for the Internet of Things (IoT)," IEEE Standards Association, accessed July 23, 2018, http://grouper.ieee.org/groups/2413/.

[205] "ITU-T Recommendations," ITU Telecommunication Standardization Sector (ITU-T), accessed July 23, 2018, https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx. For a list, see: https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/exec-sum-may18.aspx.

[206] "List of Member States," International Telecommunications Union, accessed September 6, 2018, https://www.itu.int/online/mm/scripts/gensel8.

[207] "List of Sector Members," International Telecommunications Union, accessed September 6, 2018, https://www.itu.int/online/mm/scripts/gensel11.

While many of these major organizations collaborate on initiatives and white papers, other organizations coordinate between these bodies, like the World Standards Cooperation (WSC), which promotes collaboration between the ISO, IEC, and ITU. Major standards developing organizations also work together on standalone papers and projects, like when the IEEE Standards Association, Alliance for the Internet of Things Innovation (AIOTI), oneM2M, and World Wide Web Consortium (W3C) released a joint white paper on semantic interoperability for the IoT.[208]

The varying pre-eminence of each of these organizations correlates to different visions for global standards-setting, most notably at the level of multi-stakeholder participation. Europe, for example, has moved more toward the ISO and IEC system, which offer a one-country, one-vote model of participation, whereas the United States has based its standards on participation of individual experts worldwide.[209] China, with its focus on centralized bureaucracy and coordination, also favors a one-country, one-vote model of participation, and champions the nation-state as the primary force for influence, a model it can use to its advantage by converting the nations along the Belt and Road to its standards and convincing them to vote as a block. This is particularly effective in the ITU, a venue the United States has tended to eschew as seen in the table above. While some in the United States have advocated against the ITU, China has made important inroads in recent years, with one consulting firm noting that "Even the decision by the ITU to refer to 5G by the name of IMT-2020 was considered another small win for the Chinese government who had recommended it."[210]

The competition over which stakeholders are accorded the authority to set global standards masks a deeper contest over the role of nation-states in internet governance and control. Like China, Arab states have pushed to move control of the internet into the hands of the ITU, eschewing the multi-stakeholder model encompassing business, civil society, and technical experts and instead strengthening the role of governments. A 2014 proposal from 22 Arab states to the ITU would have made "policy authority for international internet-related public policy issues" the "sovereign right of states," a viewpoint that correlates closely with China's own push for the concept of "cyber sovereignty" and a multilateral model of internet governance.[211]

United States IoT Standardization Efforts

The U.S. approach to IoT and 5G standardization tends toward free-market competition and a bottom-up multi-stakeholder model of standardization. The United States has no unified government body overseeing domestic IoT or 5G standards, and instead relies on a patchwork of governmental and industry guidelines for self-regulation at home. International standardization has in the past typically been left to U.S. companies to sort out with their European rivals, though

[208] IEEE Standards Association, AIOTI, oneM2M and W3C Collaborate on Joint White Paper Covering Semantic Interoperability for the Internet of Things (IoT)," press release, December 20, 2016, http://standards.ieee.org/news/2016/semantic_interoperability.html.

[209] Fabio Tobón, "Developing Countries and International Standardization," *ASTM Standardization News*, July 2002, https://www.astm.org/SNEWS/JULY_2002/tobon_jul02.html.

[210] "What's at Stake in China's 5G Push?" *APCO Forum*, December 14, 2016, http://apcoworldwide.com/blog/detail/apcoforum/2016/12/14/whats-at-stake-in-chinas-5g-push.

[211] Dan Levin, "At U.N., China Tries to Influence Fight over Internet Control," *New York Times*, December 16, 2015, https://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.html.

in recent years the U.S. presence in some international standards organizations has been diminishing, and representation in international standards organizations is increasingly tilting toward China and other Asian powers.

Much as there is no unified legal framework to regulate security standards for U.S. IoT devices, there is also no single government entity to define security standards for the IoT. Instead, the IoT industry is regulated through a patchwork of overlapping federal authorities. The Food and Drug Administration, the Federal Communications Commission, the Federal Trade Commission and the National Highway Traffic Security Administration, among others, all have some degree of jurisdiction over the IoT.[212] This lack of singular jurisdiction has hindered efforts to unify security standards across the IoT industry. Additionally, federal agencies lack the necessary legislative authority to mandate that device manufacturers follow security best practices.[213] As a result, federal regulations are mostly reactive, and focus on punishing firms that fail to adequately safeguard data.[214] According to one FTC attorney adviser, current IoT regulation is very "post hoc… [the FTC] wouldn't be setting a role [sic] about how people should update their devices. [It] would bring a case against [companies] who failed to do that in a reasonable manner."[215]

Since no comprehensive framework exists to regulate IoT security standards, many firms have begun to rely on the National Institute of Standards and Technology (NIST) Cybersecurity Framework to reduce their security exposure.[216] The Framework provides a roadmap of "standards, guidelines, and best practices to manage cybersecurity-related risk," including guidelines for IoT devices, and has received extensive input from both government agencies and industry stakeholders.[217] NIST also has created a comprehensive lexicon of IoT-related terms, in order to create a unified technical terminology across all industries that use IoT devices.[218] However, adherence to the NIST framework is voluntary, and cannot be uniformly applied to all IoT vendors. The framework is, at best, a stop-gap measure in the absence of comprehensive legislation.

U.S. Standardization Efforts Abroad

The United States has pursued a strategy that relies on private industry to lead its international standards-setting efforts, "supplemented by federal government contributions to discrete standardization processes," monitored by the Department of Commerce.[219] U.S. pre-eminence in technology development has for many years meant that the United States has essentially set global technical standards, but this has meant that the United States has often used this *de facto* standards-setting power in place of participating in global standards development. This disregard for international standardization activities means that, according to an OECD review of regulatory

[212] Ravindranath, "Regulating the Internet of Things."
[213] Ravindranath, "Regulating the Internet of Things."
[214] Ravindranath, "Regulating the Internet of Things."
[215] Ravindranath, "Regulating the Internet of Things."
[216] Tara Swaminatha, "The Rise of the NIST Cybersecurity Framework," *CSO Online*, May 11, 2018, https://www.csoonline.com/article/3271139/data-protection/the-rise-of-the-nist-cybersecurity-framework.html.
[217] Swaminatha, "The Rise of the NIST Cybersecurity Framework"; "Cybersecurity Framework," National Institute of Standards and Technology, accessed May 21, 2018, https://www.nist.gov/cyberframework.
[218] Ravindranath, "Regulating the Internet of Things."
[219] Dong Geun Choi and Erik Puskar, "NISTIR 8007: A Review of U.S.A. Participation in ISO and IEC," U.S. Department of Commerce National Institute of Standards and Technology (NIST), June 2014, http://dx.doi.org/10.6028/NIST.IR.8007.

reform in the United States, some international standards "have been developed without adequate US input or representation," to the detriment of U.S. competitiveness.[220]

The U.S. government itself has bemoaned for decades the lack of participation in global standardization, dating at least to 1964, when an Assistant Secretary of Commerce for Science and Technology warned that the United States refrained from international standards participation at its own economic peril.[221] A 2000 NIST review of participation in international standards bodies argued that the statement remained true, and that in the need to improve U.S. involvement in international standardization activities remained as important as ever.[222] In reports charting private-sector participation in international standards bodies from 1966 to 2012, the U.S. Chamber of Commerce has consistently noted that since the U.S. strategy relies on voluntary private-sector participation and means that involvement and willingness to pay the costs of participating depends on whether industries' perceived interests in the standards. As a result, some companies and industries have been active, but others have not participated at all.[223] Other efforts toward regulatory reform cite the difficulty U.S. trading partners have had with the complexity of the U.S. standards system, "what is perceived as an extremely complex combination of public and private, federal and sub-federal responsibilities, lacking a single co-ordination agent."[224]

International Standards Organization Participation

Despite this uneven participation, the United States has been part of major telecommunications standards efforts. Many major U.S. companies are able to credibly participate in international standard-setting organizations by virtue of their ownership of advanced core technologies needed for the IoT and 5G deployment. Companies have contributed to both the ITU and 3GPP in their efforts to develop 5G networks. For instance, U.S. telecommunications giant Qualcomm currently holds the most global 5G patents,[225] and is a world leader in mobile hardware and processors needed for IoT deployment. U.S. companies continue to maintain a presence on most 3GPP standards drafting committees, including two of the three active technical specifications groups (the plenary committees for TSG RAN (Radio Access Network) and TSG SA (Service and System

[220] Organisation for Economic Co-operation and Development (OECD), *Regulatory Reform in the United States* (Paris: OECD, 1990), 240.

[221] A 1988 U.S. Department of Commerce review of U.S. participation in international standards bodies cited the assistant secretary's comments as a "self-fulfilling prophecy," while a 2000 NIST update to the report echoed the warning. See: Patrick W. Cooke, "A Review of U.S. Participation in International Standards Activities," U.S. Department of Commerce National Bureau of Standards, January 1988, https://www.gpo.gov/fdsys/pkg/GOVPUB-C13-1758b67213d23ed7afde26884cfb4953/pdf/GOVPUB-C13-1758b67213d23ed7afde26884cfb4953.pdf; Christine R. DeVaux, "NISTIR 6492: A Review of U.S. Participation in the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)," U.S. Department of Commerce National Institute of Standards and Technology (NIST), February 2000, https://www.nist.gov/sites/default/files/nistir_6492reviewofusparticip_isoiec_2000.pdf.

[222] Cooke, "U.S. Participation in International Standards; DeVaux, "NISTIR 6492."

[223] Cooke, "U.S. Participation in International Standards; DeVaux, "NISTIR 6492"; Choi and Puksar, "NISTIR 8007."

[224] OECD, 240.

[225] Deng Xianlai and Huang Kun, "Commentary: China Catches up in Global Race to Usher in 5G Era," Xinhua (新华), March 3, 2018, http://www.xinhuanet.com/english/2018-03/02/c_137011303.htm; U.S.-China Economic and Security Review Commission, *Hearing on "China, the United States, and Next Generation Connectivity,"* March 8, 2018 (Written Testimony of Doug Brake), http://www2.itif.org/2018-testimony-china-5g.pdf.

Aspects)).[226] Qualcomm has contributed to at least one ITU document on how to implement a transition from existing LTE networks to full 5G deployments.[227]

NIST conducts regular reviews of U.S. participation in the ISO and IEC in particular, indicating that the U.S. government regards activity in those two bodies as a general proxy for U.S. participation in international standardization activities writ large. As of September 6, 2018, the United States places sixteenth out of the 162 total ISO members with participation in 593 technical committees, which is a drop from 2012 when the United States ranked twelfth with participation in 620 technical committees. Meanwhile, China has increased its participation, tying for third overall and participating in 733 technical committees, up from 706 in 2012 (See Table 5 and Table 6).[228]

Beyond general participation, NIST makes clear the additional advantages that accrue to the United States from holding secretariat positions within technical committees, which give the United States the ability to incorporate certain technologies into standards, promote the development of standards that reflect domestic interests, and ensure that the United States is represented in standards discussions.[229]

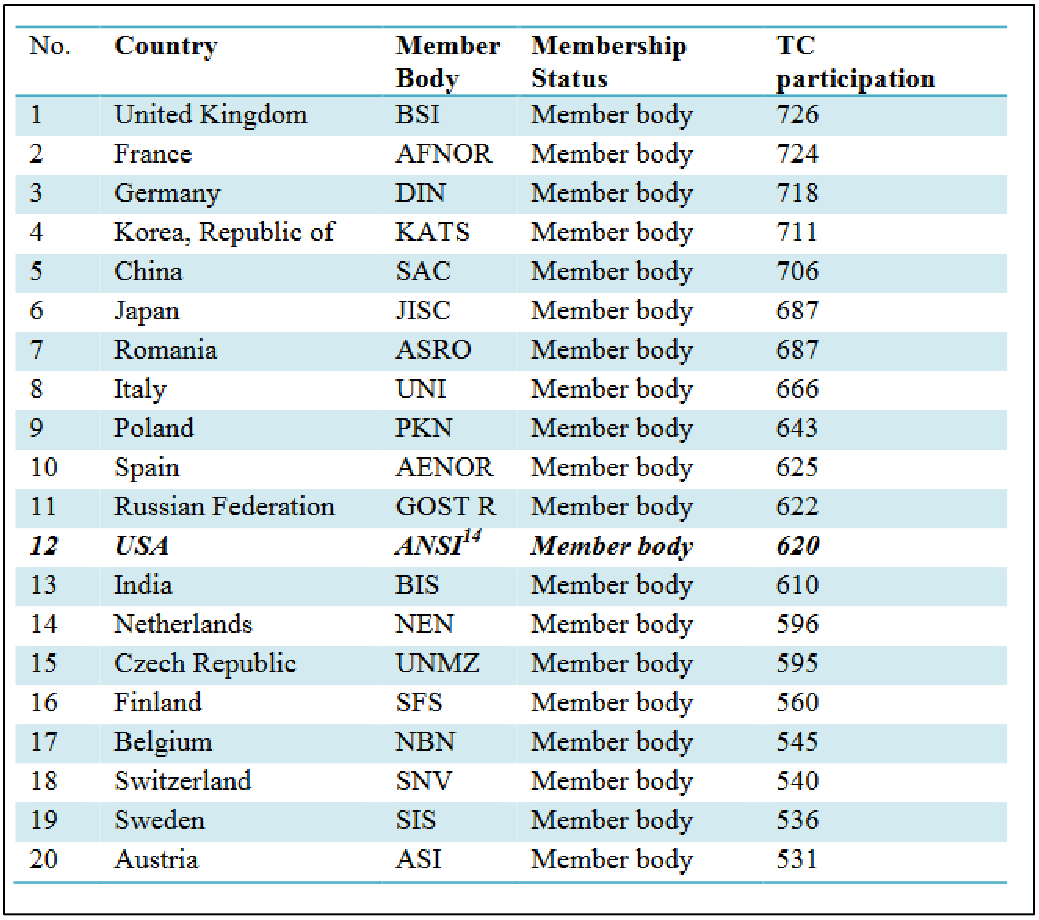
[226] "3GPP Officials for Group: 3GPP RAN ("RP")," 3GPP, accessed May 23, 2018, http://www.3gpp.org/DynaReport/TSG-WG--RP--officials.htm?Itemid=268; "3GPP Officials for Group: 3GPP SA ("SP")," 3GPP, accessed May 23, 2018, http://www.3gpp.org/dynareport/TSG-WG--SP--officials.htm?Itemid=473.
[227] "The Technological Path from LTE to 5G," 1st ITU Inter-Regional Workshop on WRC-19 Preparation," ITU, November 20, 2017, https://www.itu.int/dms_pub/itu-r/md/15/wrc19prepwork/c/R15-WRC19PREPWORK-C-0017!!PDF-E.pdf.
[228] These figures were obtained from data accessed on July 19, 2018 at https://www.iso.org/members.html. See also Choi and Puksar, "NISTIR 8007."
[229] DeVaux, "U.S. Participation in the ISO and the IEC."

Table 5: Top 20 ISO Technical Committee Participants, 2018[230]

No.	Country	Member Body	Membership Status	Technical Committee Participation	Policy Development Committee Participation
1	France	AFNOR	Member body	741	5
2	United Kingdom	BSI	Member body	735	5
3	Germany	DIN	Member body	733	5
3	**China**	**SAC**	**Member body**	**733**	**5**
5	Korea, Republic of	KATS	Member body	726	5
6	Japan	JISC	Member body	715	5
7	Italy	UNI	Member body	691	4
8	Czech Republic	UNMZ	Member body	688	4
9	Romania	ASRO	Member body	680	4
10	India	BIS	Member body	654	4
11	Russian Federation	GOST R	Member body	649	5
12	Spain	UNE	Member body	646	4
13	Poland	PKN	Member body	634	4
14	Iran, Islamic Republic of	ISIRI	Member body	616	4
15	Netherlands	NEN	Member body	610	4
16	**United States**	**ANSI**	**Member body**	**595**	**5**
16	Finland	SFS	Member body	595	5
18	Switzerland	SNV	Member body	563	5
19	Sweden	SIS	Member body	560	5
20	Belgium	NBN	Member body	542	3

[230] These figures were obtained from data accessed on September 6, 2018 at https://www.iso.org/members.html.

Table 6: NIST Report Ranking 2012 ISO Participating Countries[231]



No.	**Country**	**Member Body**	**Membership Status**	**TC participation**
1	United Kingdom	BSI	Member body	726
2	France	AFNOR	Member body	724
3	Germany	DIN	Member body	718
4	Korea, Republic of	KATS	Member body	711
5	China	SAC	Member body	706
6	Japan	JISC	Member body	687
7	Romania	ASRO	Member body	687
8	Italy	UNI	Member body	666
9	Poland	PKN	Member body	643
10	Spain	AENOR	Member body	625
11	Russian Federation	GOST R	Member body	622
12	***USA***	***ANSI***[14]	***Member body***	***620***
13	India	BIS	Member body	610
14	Netherlands	NEN	Member body	596
15	Czech Republic	UNMZ	Member body	595
16	Finland	SFS	Member body	560
17	Belgium	NBN	Member body	545
18	Switzerland	SNV	Member body	540
19	Sweden	SIS	Member body	536
20	Austria	ASI	Member body	531

The United States has tended to accord less importance to the ITU, a treaty organization for which the Department of State coordinates U.S. participation.[232] Some have argued the ITU hovers on the verge of irrelevance[233] and is "woefully out of step with the most technologically advanced sectors of the global society,"[234] a view more common in the United States as U.S. companies moved into new technological frontiers. In addition, the ITU overall and the ITU-T in particular have a lackluster track record when it comes to addressing network security. U.S.-based standards expert and ITU cybersecurity lead Anthony Rutkowski[235] argued in 2012 that "ITU as an

[231] Choi and Puksar, "NISTIR 8007."

[232] Choi and Puksar, "NISTIR 8007."

[233] Geoff Huston, "Opinion: ICANN, the ITU, WSIS, and Internet Governance," *The Internet Protocol Journal* 8 (1), https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-31/internet-governance.html.

[234] Elise Ackerman, "The U.N. Fought the Internet–And the Internet Won; WCIT Summit in Dubai Ends," *Forbes*, December 14, 2012, https://www.forbes.com/sites/eliseackerman/2012/12/14/the-u-n-fought-the-internet-and-the-internet-won-wcit-summit-in-dubai-ends/.

[235] "Anthony Rutkowski," American Bar, accessed July 23, 2018, https://www.americanbar.org/content/dam/aba/administrative/law_national_security/patriots_debate/author_bios/Bio_Rutkowski.authcheckdam.pdf.

institution has not possessed in modern history, and today does not possess the competence to deal with the subject matter of network security."[236]

U.S. objections to the ITU leads to something of an oppositional positioning between ITU as the leader of the multilateral, UN-driven model and ICANN, the U.S.-based multi-stakeholder nonprofit created to manage the Internet Assigned Numbers Authority (IANA).[237] Expanding the role of the ITU, as China and others would like to do, would also mean taking responsibility away from specialized U.S.-based organizations like the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C).[238]

One indication of these efforts to expand the ITU's role came in the 2015 creation of the ITU's Telecommunication Standardization Sector's (ITU-T) Study Group 20. The group was created over the objections of the United States and others to focus on developing international IoT standards.[239] The objectors argued that expanding the ITU's work agenda[240] exceeded the organization's mandate and at best duplicated and at worst renders ineffective existing private sector-led global standardization efforts through other standards development organizations.[241] There are no rapporteurs and only one management team representative from the United States (affiliated with NTIA),[242] in keeping with what some have observed as the absence of many U.S. stakeholders in important standards groups,[243] and with lower U.S. enthusiasm for the ITU as a standards-setting venue.

[236] Anthony Rutkowski, "A Short History of ITU Network Security Activity," *CircleID*, October 1, 2012, http://www.circleid.com/posts/20121001_a_short_history_of_itu_network_security_activity/.

[237] Phillip Hallam-Baker, "The Geo-Politics of ICANN vs ITU," *CircleID,* July 20, 2010, http://www.circleid.com/posts/the_geo_politics_of_icann_vs_itu/.

[238] Declan McCullagh, "The U.N. Thinks about Tomorrow's Cyberspace," *CNet*, March 29, 2005, https://www.cnet.com/news/the-u-n-thinks-about-tomorrows-cyberspace/.

[239] "Study Group 20 at a Glance," ITU-T, accessed May 23, 2018, https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

[240] "Study Group 20 at a Glance," ITU-T, accessed May 23, 2018, https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx; "Mandate and Lead Roles: Study Group 20 (Study Period 2013-2016)," ITU-T, accessed July 23, 2018, https://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/mandate.aspx.

[241] David A. Gross, "Internet Governance in Transition: The ITU as a Battleground for Rival Visions," *CircleID*, April 29, 2016, http://www.circleid.com/posts/20160429_internet_governance_in_transition_itu_battleground_rival_visions/; Jacquelynn Ruff, Leslie J. Martinkovics, and Ian Dillner, "Comments of Verizon," In the Matter of Telecommunication Standardization Assembly, Department of Commerce National Telecommunications and Information Administration (NTIA), June 16, 2016, https://www.ntia.doc.gov/files/ntia/publications/2016_06_16_verizon_comments_on_ntia_wtsa-16_conference.pdf; "ITU WTSA 2016 Outcomes: An Internet Society Perspective," Internet Society, November 22, 2016, https://www.internetsociety.org/resources/doc/2016/itu-wtsa-2016-outcomes-an-internet-society-perspective/.

[242] "SG20: List of Questions and Rapporteurs (Study Period 2017-2020)," ITU-T, accessed July 23, 2018, https://www.itu.int/net4/ITU-T/lists/loqr.aspx?Group=20&Period=16.

[243] Nicole Blanchard, "How ITU, 5GPPP, NGMN and Others Will Create the Standard for 5G," *Fierce Wireless,* accessed July 23, 2018, https://www.fiercewireless.com/special-report/how-itu-5gppp-ngmn-and-others-will-create-standard-for-5g.

U.S. Private-Sector Standardization Efforts

There is little centralized coordination among standards stakeholders in the United States, or between major U.S. companies when they engage in standardization efforts for IoT and 5G beyond U.S. shores. Much of the existing influence of U.S. companies is derived from U.S. intellectual property ownership in core IoT technologies, the continued widespread usage of U.S. products around the world, and ongoing cooperation between U.S. and foreign companies in testing new technologies. Given this traditional advantage, U.S. companies are motivated to get new technologies and products to market first, ensuring widespread use and the effective adoption of U.S. IPR as part of the global standard.

In an effort to lead and keep pace with global technological developments, U.S. mobile communications networks have moved to roll out international standard-compliant technology in a race to deploy effective 5G before their domestic rivals. Verizon, for instance, has been an early adopter of 3GPP's Release 15 standard[244] and is currently testing the standard in eleven different markets.[245]

U.S. companies are also working with foreign counterparts to test 5G in multiple areas. For example, in February 2018, U.S. carrier Verizon partnered with Qualcomm and with Finland's Nokia to reach an early 5G milestone, completing the first call on a 3GPP standard-compliant 5G New Radio system using Verizon's licensed millimeter wave spectrum.[246] This type of cooperation is not limited to Western firms, however: Qualcomm has also cooperated with Huawei to conduct 5G interoperability and development testing based on the 3GPP Release 15 standard, with Qualcomm's chipsets as a key part of Huawei's commercial system.[247] Companies have put out a flurry of press releases announcing various similar milestones: in January 2018, Intel, Deutsche Telecom, and Huawei announced the world's first successful over-the-air test demonstrating 5G interoperability and development testing based on the Release 15 NSA 5G New Radio specification.[248]

Intel, a company that also hopes to have its 5G chipsets inside Chinese devices by 2019, has been partnering with Huawei since 2017. In mid-2018, Intel partnered with Huawei and China Mobile to conduct similar 5G interoperability and development testing at China Mobile's research institute to help bring 5G commercialization. Such trials, the Intel general manager pointed out, "build the 'recipe' that Huawei can then take to carriers who build it out, while Intel takes the recipe to OEMs and ODMs." An Intel vice president noted that "Intel's collaboration with China Mobile and

[244] Release 15 is a 3GPP standard that covers "Phase 1" of the proposed 5G rollout (see: http://www.3gpp.org/release-15). Release 16, covering "Phase 2," is planned to be finalized at the end of 2019 (see: http://www.3gpp.org/release-16).

[245] Mike Dano, "AT&T, Verizon both Promise to be 'First' with 5G," *FierceWireless*, February 27, 2018, https://www.fiercewireless.com/5g/at-t-verizon-both-promise-to-be-first-5g.

[246] "Another Step toward Mobile 5G Service: Verizon, Nokia and Qualcomm Complete First Call Using 3GPP-Compliant 5G New Radio Technology," Verizon Communications (press release), February 12, 2018, https://globenewswire.com/news-release/2018/02/12/1339484/0/en/Another-step-toward-mobile-5G-service-Verizon-Nokia-and-Qualcomm-complete-first-call-using-3GPP-compliant-5G-New-Radio-technology.html.

[247] "Qualcomm and Huawei Successfully Complete 3GPP-Based 5G Interoperability Testing," Qualcomm (press release), February 18, 2018, https://www.qualcomm.com/news/releases/2018/02/21/qualcomm-and-huawei-successfully-complete-3gpp-based-5g-interoperability.

[248] "Intel Enables World's First Fully Compliant Testing of New 5G NR Standard for Deutsche Telecom and Huawei," Intel (press release), January 25, 2018, https://newsroom.intel.com/news/intel-enables-worlds-first-fully-compliant-testing-new-5g-nr-standard-deutsche-telecom-huawei/.

Huawei will help accelerate the future of 5G," and commented how China is set to be an early leader in 5G.[249]

China's Push to Set IoT Standards

Formulating and promoting official standards is regarded as a critical tool for improving product quality and safety while increasing profits and economic growth through better coordination and interoperability.[250] These themes are not unique to China: economists and standardization experts around the world agree that standardization achieves all of those goals when executed successfully.[251] Where China is unique is in the priority it has given to a national standards strategy and in the multi-faceted effort it is using to push for widespread adoption of its preferred technical standards internationally. China's desire to influence international standards touches on a larger contest about intellectual property ownership, market advantage, international prestige, and approaches to privacy, security, and control of data.

China push to set international standards for emerging technologies is part of its overall strategy to become a global science and technology powerhouse and move up the production value chain, especially for IoT and 5G technology. China's quest for pre-eminence in these fields comes with government backing, both in support to "national champions"[252] as they seek to set *de facto* standards by developing innovative technologies and in promoting increased Chinese representation in international standards organizations. In addition, China seeks cooperative relationships with other nations that will help it influence global technical standards.

In the past, China made several mostly unsuccessful attempts to promote domestic standards globally like the TD-SCDMA 3G mobile cellular standard and WAPI wireless LAN standards, learning lessons that have allowed the country to position itself to launch more successful efforts in the future.[253] While these past attempts did not resulted in widespread international adoption,

[249] Corinne Reichert, "Huawei, Intel, China Mobile Complete 5G Interoperability Testing," July 10, 2018, ZDNet, https://www.zdnet.com/article/huawei-intel-china-mobile-complete-5g-interoperability-testing/.

[250] In Chinese: "党中央、国务院高度重视标准化工作，2001 年成立国家标准化管理委员会，强化标准化工作的统一管理。" State Council of the People's Republic of China, "国务院关于印发深化标准化工作改革方案的通知" (Notice of the State Council on Printing and Distributing the Reform Plan for Deepening Standardization Work), March 26, 2015, http://www.gov.cn/zhengce/content/2015-03/26/content_9557.htm.

[251] See, for example, "Economic Benefits of Standardization," DIN German Institute for Standardization, April 2000, https://www.iec.ch/about/globalreach/academia/pdf/academia_governments/economic_benefits_standardization.pdf, and an updated version, Knut Blind, Andre Jungmittag, and Axel Mangesldorf, "Economic Benefits of Standardization," DIN German Institute for Standardization, June 2011, https://www.din.de/blob/89552/68849fab0eeeaafb56c5a3ffee9959c5/economic-benefits-of-standardization-en-data.pdf.

[252] So-called "national champions" enjoy state support through preferential policies, access to financing, and other perks designed to promote their growth.

[253] Steven Schwankert, "3G in China: One Country, Three Standards," *PC World*, September 11, 2008, https://www.pcworld.com/article/150985/article.html; Bo Li, Dongliang Xie, Shiduan Cheng et al., "Recent Advances on TD-SCDMA in China," *IEEE Communications Magazine* 43 (1) (January 2005): 30-37, https://ieeexplore.ieee.org/document/1381872/; In Chinese, "此前，国家科技部办公厅调研室也在一份调研报告中，对 WAPI 问题进一步作出评论，'中国与美国在 WAPI 问题上的较量，完全是国家利益之间博弈的过程。遗憾的是，我们失败了'。" Zhang Aijing, ed., "科技部全面剖析 WAPI 失败原因及中国标准战略" [Ministry of Science and Technology Comprehensively Analyzes the Reasons for WAPI's Failure and China's

they benefited China by offering a competitive standard, a tactic that "pushes foreign standards alliances to lower royalty rates."[254] Going forward, China has worked to ensure that its standards win wider adoption and that its companies not only pay lower royalty rates but have the chance to earn substantial royalty revenues.

China's effort to set international IoT standards starts at home. Emphasis on standard-setting has increased since the 19th National Congress of the Communist Party of China, which declared China's economy had shifted from "a high-speed growth stage" to "a high-quality development stage."[255] Standards were singled out as "especially important" in this transition. Xi Jinping has been widely quoted in saying that "standards determine quality," and that it is possible to achieve "high quality only with high standards."[256] This is indicative of the central role the Chinese government sees for standardization at home and abroad, from which its other initiatives flow. In its domestic standardization work, China has revised law and begun new studies and initiatives to modernize and promote standardization.

Domestic Standardization: More than Tech Specs

China's domestic standardization efforts originally focused on improving product quality in state production quotas, which resulted in standards of limited relevance driven more by political mandate than technological reality. More recent standardization efforts, however, have emphasized the protection of national security and the fostering of Chinese economic strength in the global market.

China's efforts to modernize its domestic standardization work have accelerated in recent years. The 2018 revision to the 1988 Standardization Law of the People's Republic of China[257] aimed at simplifying and increasing the influence of the market in the standards-setting process while also raising the profile of Chinese standards globally,[258] a goal toward which all levels of government are expected to work. Article 3 of the law defines "standardization work" to include "developing standards, organizing the implementation of standards, and overseeing the development and implementation of standards" and notes that "People's Governments at or above the county level

Standards Strategy], *People's Daily Online 人民网*, August 17, 2004, http://www.people.com.cn/GB/guandian/35560/2715892.html.

[254] Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions," report prepared for the U.S.-China Economic and Security Review Commission, January 16, 2013, https://www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf; Thomas Hout and Pankaj Ghemawat, "China vs. the World: Whose Technology Is It?" *Harvard Business Review* (December 2010), https://hbr.org/2010/12/china-vs-the-world-whose-technology-is-it.

[255] "Tian Shihong: Solidly Conducting Standardization and Helping Quality Improvement Work," *中国质量报* [*China Quality News*], November 2017, http://samr.aqsiq.gov.cn/ztlm/2017/zltsxd/wjjd/201711/t20171120_502770.htm.

[256] In Chinese: "标准决定质量，有什么样的标准就有什么样的质量，只有高标准才有高质量。" In: "Tian Shihong," *China Quality News*.

[257] "Standardization Law of the People's Republic of China (Full Text)," Standardization Administration of the People's Republic of China, January 2, 2018, http://202.99.59.128/sacen/law/201801/t20180102_340493.htm.

[258] Deutsches Institut für Normung (DIN, German Institute for Standardization), "China's Standardization Reform," August 2017, https://www.din.de/blob/257494/ee0b06981acdd9e0e9ac342ff5f40b1a/china-s-standardization-reform-data.pdf.

shall incorporate standardization work in their economic and social development plans, and include relevant expenditure in their budget."[259]

China's standardization is focused on modernizing its industry and helping the country become an international standards-maker rather than a standards-taker, but it is never far removed from other national objectives, like national security. Article 23 of the revised Standardization Law makes this intent clear:

- The State shall promote standards that encourage civil-military integration and resource sharing, increase the harmonization of civil and military standards, and promote the use of advanced and appropriate civilian standards in the development of national defense and the military, and it shall convert advanced and appropriate military standards into civilian standards.[260]

Beyond revising the national law, in 2018 the Chinese government also initiated the "China Standards 2035" project (中国标准 2035), a two-year collaborative study under the auspices of the Standards Administration of China (SAC) and the General Administration of Quality Supervision, Inspection and Quarantine (AQSIQ) with implementation entrusted to the Chinese Academy of Engineering, a national think tank under the State Council.[261] Among its aims, the project hopes to speed up the formulation and implementation of China's standardization strategy and the domestic and international standards mutual recognition project. Much like the Standardization Law, the project also includes a civil-military integration push: one of the four major topics of the China Standards 2035 project is "Research on Standardization of Military and Civil Integration Development Strategy."[262]

ICT, especially the IoT, figure prominently in specific standards-setting initiatives and discussion of standards internationalization. A news article announcing the undertaking of the "China Standards 2035" project quoted a deputy director of MIIT speaking about the ministry's plans to continue standardization and internationalization work, in particular focusing on promoting Chinese national and industry standards in the fields of the IoT, information technology equipment interconnection, and solar photovoltaics to become international standards.[263]

[259] "Standardization Law of the People's Republic of China (Full Text)."

[260] "Standardization Law of the People's Republic of China (Full Text)."

[261] "'Chinese Standards 2035' Project Launched in Beijing," Standardization Administration of the People's Republic of China, March 8, 2018, http://202.99.59.128/sacen/events/201803/t20180308_341856.htm.

[262] In Chinese: "标准化军民融合发展战略研究." In: "中国标准 2035" 项目在京启动: 项目计划 2020 年结题形成项目报告并向党中央国务院提出实施标准化战略的建议" [China Standards 2035 Project Launched in Beijing: The Project Plans to Finalize Project Report in 2020 and Issue Proposals to the Party Central Committee and State Council to Implement the Standardization Strategy], General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, March 2, 2018, http://www.aqsiq.gov.cn/zjxw/zjxw/zjftpxw/201803/t20180302_513610.htm.

[263] In Chinese: "工业和信息化部电子信息司副司长乔跃山表示，将持续加强标准化与国际化工作，推动物联网、信息技术设备互联、太阳能光伏等领域的国家标准或行业标准成为国际标准，加快转化我国产业发展急需的国际先进标准，推动国内外标准接轨。" In: "《中国标准 2035》将发布" ["'China Standards 2035' Will Be Released"], Government of the People's Republic of China, January 11, 2018, http://www.gov.cn/xinwen/2018-01/11/content_5255443.htm.

Centrally Planned Standards: The Standardization Administration of China

China's current domestic standardization efforts are part national rejuvenation through economic development and national security and part central economic planning. Nationwide standardization efforts in nearly every sector of the economy are overseen by the Standardization Administration of China (中华人民共和国国家标准化管理局, also known as 国家标准化管理委员会; SAC).[264] The SAC is the sole administration under the State Council authorized to carry out standardization work in the pursuit of "improving quality of products and services, promoting scientific and technological improvement…and protecting national security and improving socioeconomic standards,"[265] though standards in select specialized fields like aerospace and environmental protection are administered by their respective ministries.[266]

Searches of authoritative SAC public standards databases for terms including "Internet of Things (物联网)" and "smart (智能)" from 2001 to 2017 yielded 117 National Standards currently in effect (现行) or about to be implemented (即将实施). All but seven of these are recommended standards and the outstanding seven were guiding standards covering smart grid technologies–none were mandatory documents.[267]

National-level IoT standards have been disseminated at an increasing pace. Available data from SAC databases indicate that the number of IoT and smart product standards began to inch upwards in 2015 and spiked in 2017, although the precise rationale for the timing of the increase remain unclear.[268] A similarly prominent trend is obvious in the adoption and implementation of these standards, with the caveat that a substantial proportion of the 2018 standards are scheduled for implementation and not fully enacted at the time of writing. The figure below shows these trends.

[264] Standardization Administration of the People's Republic of China, "标准委介绍" [Standardization Committee Description], July 12, 2007, http://www.sac.gov.cn/sxxgk/bzwjs/201012/t20101210_56512.htm.

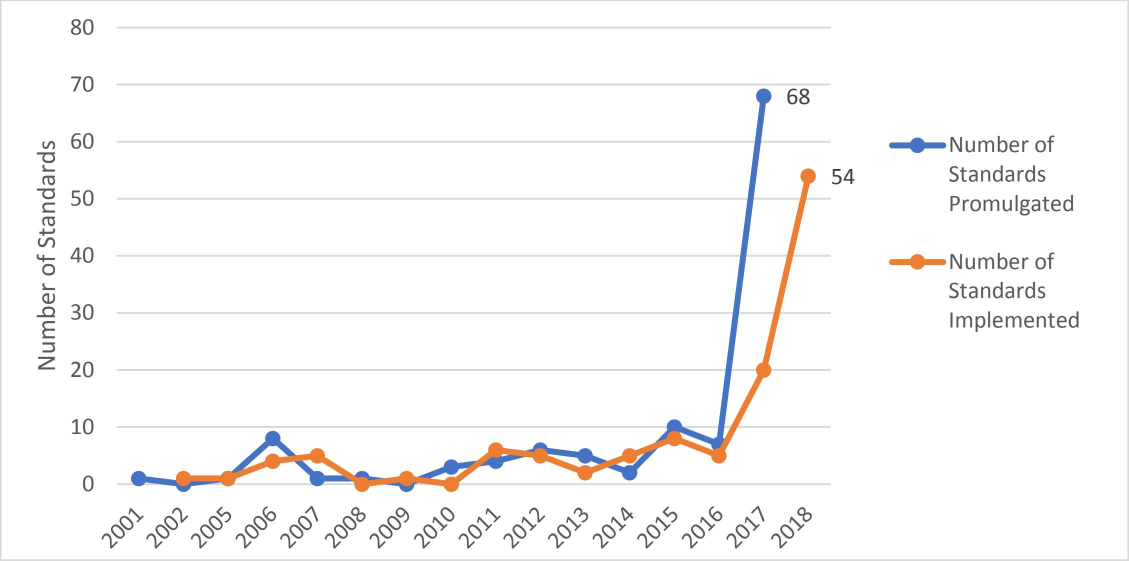
[265] National People's Congress of the People's Republic of China, "中华人民共和国标准化法" [Standardization Law of the People's Republic of China], November 4, 2017, http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031446.htm.

[266] Deutsches Institut für Normung (DIN), "China's Standardization Reform."

[267] These figures are derived from information retrieved from various official standards databases. Standards information can be found at Standardization Administration of China 中国国家标准化管理委员会, "国家标准信息查询" [National Standards Information Query], accessed on May 17, 2018, http://www.aqsiq.gov.cn/zhcx/index_6530.htm.

[268] The SAC apparently felt that a more robust regulatory response to overall Chinese IoT development was needed, but the precise reasons for the timing of the spike are somewhat unclear. Possible explanations for the exact timing could include the cyclical nature of standards production, a clearing of a bureaucratic logjam, or the issuance of a top-down mandate to approve and issue more standards.

Figure 3: Number of IoT and Smart Standards Promulgated and Enacted (or About to Be Enacted), 2001-2018[269]



As standards for IoT and "smart (智能)" products have proliferated, so too have the number of organizations and people that have accompanied the effort. The drafting processes behind the 117 National Standards identified in this report was helmed by some 30 different technical committees (TC), and some 576 government agencies, research institutes, universities, and state and privately-run companies participated in drafting these IoT and smart product standards.[270]

Key Industries for Domestic IoT Standardization

China's IoT standardization efforts have thus far emphasized industries like smart transportation, industrial process management, electrical power grids, information technology, and information security. Some of this emphasis is a direct reflection of Beijing's broader economic planning priorities, especially information technology and information security.[271] The most prolific participants in the leadership and drafting of the National Standards identified in this chapter are all government agencies or companies with close government ties, as shown in Table 7.

Almost all of the major standardization organizations identified in the data have direct ties to international standardization bodies. For some, these ties are openly stated: for instance, TC 268, the technical committee focused on smart transportation is described as a direct counterpart to the International Organization for Standardization committee on intelligent transport systems (ISO/TC

[269] These figures are compiled from information retrieved from various official standards databases. Standards information can be found at Standardization Administration of China 中国国家标准化管理委员会, "国家标准信息查询" [National Standards Information Query], accessed on May 17, 2018, http://www.aqsiq.gov.cn/zhcx/index_6530.htm.

[270] These statistics are derived from data collected from various SAC databases. See Standardization Administration of China 中国国家标准化管理委员会, "国家标准信息查询" [National Standards Information Query], accessed on May 17, 2018, http://www.aqsiq.gov.cn/zhcx/index_6530.htm.

[271] See Chapter 1 and Chapter 3 for more on Beijing's emphasis on information technology and security, respectively.

204).[272] The technical committee for information technology, TC 28, is described as a direct counterpart to the International Organization for Standardization committee on information technology (ISO/IEC JTC 1).[273]

[272] "标委会简介" [Committee Summary], National Technical Committee 268 on Intelligent Transport Systems of SAC 全国智能运输系统标准化技术委员会, accessed May 17, 2018, https://web.archive.org/web/20131226064114/http://www.its-standards.cn:80/abuot/index.asp.

[273] "全国信息技术标准化技术委员会" [National Information Technology Standardization Technical Committee], Standards Management and Service Center 标准管理与服务中心, March 17, 2017, http://www.cesi.ac.cn/201703/2264.html.

Table 7: Major Participants in Chinese IoT Standardization Efforts

English Name or Designator	Chinese Name	Organizational Affiliations	Primary Area of Expertise	Number of Standards Led or Drafted
TC 124	全国工业过程测量控制和自动化标准化技术委员会	SAC, MIIT, China Machinery Industry Federation (中国机械工业联合会)[274]	Industrial control, automation, communication, industrial computing, control instrumentation[275]	26 (Led)
TC 268	全国智能运输系统标准化技术委员会	SAC, Ministry of Transportation[276]	Surface traffic management, advanced public transportation systems, among others[277]	17 (Led)
TC 28	全国信息技术标准化技术委员会	SAC, China Electronics Standardization Institute[278]	Information technology, information integration, transmission, exchange, management, organization, and storage[279]	12 (Led)
TC 260	全国信息安全标准化技术委员会	SAC, China Electronics Standardization Institute[280]	Information security, including classified information, security testing, public key infrastructure, big data security, and information management[281]	8 (Led)

[274] "标委会简介" [Committee Summary], National TC124 on Industrial Process Measurement, Control, and Automation 全国工业过程测量控制和自动化标准化技术委员会, accessed May 17, 2018, http://www.tc124.com/Gybwh.html.

[275] "标委会简介" [Committee Summary], National TC124.

[276] "标委会简介" [Committee Summary], National Technical Committee 268 on Intelligent Transport Systems of SAC 全国智能运输系统标准化技术委员会, accessed May 17, 2018, https://web.archive.org/web/20131226064114/http://www.its-standards.cn:80/abuot/index.asp.

[277] "标委会简介" [Committee Summary], National Technical Committee 268.

[278] "全国信息技术标准化网" (China National Information Technology Standardization Network), National Information Technical Standardization Committee 全国信息技术标准化技术委员会, accessed May 17, 2018, http://www.nits.org.cn/.

[279] "全国信息技术标准化技术委员会" [National Information Technology Standardization Technical Committee], Standards Management and Service Center 标准管理与服务中心, March 17, 2017, http://www.cesi.ac.cn/201703/2264.html.

[280] "领导设置" [Leadership Establishment], National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, accessed May 15, 2018, https://www.tc260.org.cn/front/tiaozhuan.html?page=/front/gywm/ldsz_Detail.

[281] "机构设置" [Organization Establishment], National Information Security Standardization Technical Committee.

China Electric Power Research Institute	中国电力科学研究院	State Grid Corporation of China[282]	R&D on high-voltage transformers, electric grid planning, power transmission engineering, and electric grid communications systems, etc.[283]	17 (Drafted)
China Electronics Standardization Institute	中国电子技术标准化研究院	MIIT[284]	Foundational standardization R&D of electronic information technology[285]	14 (Drafted)
Fujian Wide Plus Precision Instruments Co., Ltd.	福建上润精密仪器有限公司	Privately held company[286]	Live bus control systems, next-generation sensors, IoT systems, precision machining[287]	13 (Drafted)
Research Institute of Highway	交通运输部公路科学研究院	Ministry of Transportation[288]	R&D on highway, bridge, and traffic engineering; smart traffic, automobile applied engineering, traffic flow[289]	11 (Drafted)

[282] "院况介绍" [Overview and Summary of Institute], China Electric Power Research Institute 中国电力科学研究院, February 2, 2018, http://www.epri.sgcc.com.cn/html/epri/col1010000025/2012-04/01/20120401090930715168590_1.html.

[283] [Overview and Summary of Institute], China Electric Power Research Institute.

[284] "机构介绍" [Organization Summary], China Electronics Standardization Institute 中国电子技术标准化研究院, accessed May 17, 2018, http://www.cesi.cn/page/basicinfo.jsp?catalog=/001/001-001.

[285] [Organization Summary], China Electronics Standardization Institute.

[286] National Enterprise Credit Information Publicity System, "福建上润精密仪器有限公司" [Fujian Wide Plus Precision Instruments Company, Ltd.], accessed May 17, 2018, http://fj.gsxt.gov.cn/%7B291086264E7677ABA2022C141D05CBA303B0797048FBE341D7EF87279489D77759EAF250C6FE37EB80E8345F96B87149056FE94718A61B8A34B235A41A8053DCC8E1C8E1C847537AD0F9EDC4EDC4ED16331A33BC953F951A331A33F0D96200CED3A19F968E40AC82EAE3D5AD07133A35FC204B8231FFF6C04F5B725B725B-1526570705190%7D.

[287] National Enterprise Credit Information Publicity System, [Fujian Wide Plus Precision Instruments Company, Ltd.].

[288] "本院概况" [Summary of Institute], Research Institute of Highway 交通运输部公路科学研究院, accessed May 17, 2018, http://www.rioh.cn/Stencil/002/gywm.asp?xcd=2.

[289] [Summary of Institute], Research Institute of Highway.

Ties to China's Internal Security and Intelligence Services

At least one of the technical committees described in Table 7 has extensive ties to China's internal security and intelligence apparatuses. Much of TC 260's leadership has ties to various internal security and intelligence organizations: for instance, the director (主任委员) of the committee hails from the CCP Central Committee Office of the Leading Small Group for Internet Security and Informatization (中央网络安全和信息化领导小组办公室), more commonly known as the Cyberspace Administration of China (CAC), which is responsible for coordinating internet surveillance and censorship in China. [290] TC 260's deputy directors are personnel seconded from CAC, the Ministry of Public Security (MPS) 11th Bureau, the China Information Technology Evaluation Center Security Testing Center (中国信息安全测评中心; CNITSEC), the State Encryption Management Bureau (国家密码管理局; SEMB), and the State Secrecy Bureau (国家保密局; SSB). The MPS 11th Bureau is responsible for internet surveillance and security;[291] CNITSEC has extensive ties to the Ministry of State Security (国家安全局; MSS), China's foreign intelligence service, and may actually be an MSS subordinate organization;[292] SEMB and SSB are responsible for securing classified materials and state secrets.[293] China's internal security and intelligence apparatuses clearly have an abiding interest in the development and standardization of the IoT, and the presence of the security state is manifested clearly in the composition of critical technical committees charged with standardizing China's IoT sector.

China's surveillance state is also involved in IoT standards at a more granular level. At least two MPS R&D organizations are prolific drafters of IoT standards: the MPS's 1st Research Institute (公安部第一研究所; MPS 1st RI) and 3rd Research Institute (公安部第三研究所; MPS 3rd RI) helped draft IoT standards governing system interface requirements, [294] IoT reference

[290] "领导设置" [Leadership Establishment], National Information Security Standardization Technical Committee 全国信息安全标准化技术委员会, accessed May 15, 2018, https://www.tc260.org.cn/front/tiaozhuan.html?page=/front/gywm/ldsz_Detail.

[291] Ministry of Public Security of the People's Republic of China, "公安部网络安全保卫局通报打击网络淫秽色情工作情况" [Ministry of Public Security Internet Security Protection Bureau Report on Attacking Salacious Pornographic Material], December 31, 2009, http://www.mps.gov.cn/n2253534/n2253535/n2253537/c4128555/content.html.

[292] CNITSEC's Communist Party Secretary Wu Shizhong (吴世忠) as of 2015 was formerly the director for the MSS Technology Bureau (科技局), and Western cybersecurity researchers have identified CNITSEC as an MSS organization. See Ministry of Civil Affairs of the People's Republic of China, "关于成立国家标准化体系建设工作机构的通知" [Notice Regarding the Establishment of National Standardization System Work Organizations], accessed May 17, 2018, http://kjbz.mca.gov.cn/article/mzbzhzcwj/201106/20110600157934.shtml; Tan Shulin 谭树森 et al., "中国信息安全测评中心书记　吴世忠" [China Information Technology Evaluation Center Security Testing Center Party Secretary Wu Shizhong], December 16, 2015, *People's Daily Online 人民网*, http://www.cac.gov.cn/2015-12/17/c_1117487279.htm; Insikt Group, "China's Cybersecurity Law Gives the Ministry of State Security Unprecedented New Powers Over Foreign Technology," Recorded Future Blog, August 31, 2017, https://www.recordedfuture.com/china-cybersecurity-law/.

[293] See "机构职责" [Organizational Responsibilities], State Encryption Management Bureau 国家密码管理局, accessed May 15, 2018, http://www.oscca.gov.cn/sca/jggk/index.shtml and "机构职责" [Organizational Responsibilities], Shanghai Secrecy Administration Bureau 上海保密局, accessed May 17, 2018, http://www.shbmj.gov.cn/bmj/2013bmj/jgzn/jggk/u1a812.html.

[294] Standardization Administration of the People's Republic of China, "国家标准查询" [National Standard Query GB/T 35319-2017], accessed May 17, 2018,

architecture,[295] and testing and evaluation approaches for smart mobile terminals,[296] among others. MPS 1st RI and 3rd RI are also responsible for developing biometric facial recognition security equipment and video surveillance equipment, among other hardware and software deployed by China's ever-expanding mass surveillance apparatus.[297]

While China's internal security and intelligence organizations have more than a passing interest in IoT standardization, the specific demands and requirements that these organizations introduce into recent IoT standards remain difficult to ascertain. Many of the most relevant IoT standards were issued in the last half of 2017 and are not yet in effect. While the role of China's internal security organizations in drafting these IoT standards is undeniable, almost all of these recent standards are drafted by multiple organizations and personnel, making it difficult to determine which specifications were introduced by which organizations.

China's domestic standardization efforts are evidently a point of emphasis for the Chinese Communist Party, including its security apparatus. Given the sheer size and the importance of the Chinese market, the widespread adoption of a domestic IoT standard in which a Chinese government security service had a drafting role could have wide-ranging consequences not just for China but also for the world, especially as Beijing increasingly pushes for its standards preferences abroad.

China's Role in International Standardization Efforts

As the largest potential market for many IoT applications, China has an inherent advantage in standards negotiations, as any standard China adopts carries the heft of the sizable Chinese economy. This advantage is magnified through a comprehensive techno-nationalist strategy that coordinates Chinese efforts to gain leading roles in international standards organizations while also using state funding to allow Chinese companies to undersell their competitors in developed economies and win infrastructure contracts in developing markets, ensuring that its indigenously-developed technologies and standards become widely adopted with or without international recognition. This coordination is evident in both state planning documents and in current Chinese efforts to set international standards and facilitate the effective adoption of its standards through expanding its technological footprint around the world.

China's latest efforts to modernize its domestic standardization processes lay the groundwork for the country's influence efforts in international standard-setting. In tandem with streamlining the standards-setting process domestically, the January 1, 2018 revision to the 1988 Standardization

http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2035319-2017%27.

[295] Standardization Administration of the People's Republic of China, "国家标准查询" [National Standard Query GB/T 33474-2016], accessed May 17, 2018, http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2033474-2016%27.

[296] Standardization Administration of the People's Republic of China, "国家标准查询" [National Standard Query GB/T34975-2017], accessed May 17, 2018, http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2034975-2017%27.

[297] See Standardization Technical Committee for Security and Protection Alarm Systems of China, "全国安全防范报警系统标准化技术委员会简介" [Standardization Technical Committee for Security and Protection Alarm Systems of China Summary], accessed May 17, 2018, http://www.tc100.org.cn/JianJie/index.asp.

Law aims to strengthen the distribution of Chinese standards across Belt and Road Initiative countries and creating a more prominent place for Chinese standards in international standards organizations.[298] Article 8 of the revised law notes that the state will encourage participation in international standardization and promote the "adoption of international standards in the Chinese context" and "harmonization of Chinese and foreign standards."[299] Article 9 ensures rewards and incentives for those that make outstanding contributions to standardization work.[300]

Further plans to influence international standards are embedded in other standardization efforts, like the "China Standards 2035" project, which hopes to speed the "mutual reconciliation of domestic and international standards." [301] The director of the Industry Standards Department II at SAC noted that the timing presents a "good opportunity to realize the transcendence of China's industry and standards" given that the "international technology research and development and patent layout have not yet been completed, and global technical standards are still being formed."[302]

Chinese state economic plans lay out corresponding specific international directives for influencing international standards. IoT-specific state plans, like the "Special Project Action Plan for Internet of Things Development" (物联网发展专项行动计划), provide further insight into the importance the Chinese government gives to influencing international standardization in IoT. The plan is divided into ten subordinate special action plans covering various aspects of IoT development. One of these subordinate special action plans is the "Special Project Action Plan for Standards Formulation" (标准制定专项行动计划; SPAPSF), which openly calls for China to dominate the ISO/IEC and ITU and expand the number of international IoT standards led by China.[303] The SPAPSF explicitly calls for the SAC, NDRC, and MIIT to coordinate with relevant departments to:

> guide Chinese IoT standards internationalization work, promote the formation of regional and international standardization organizations, become a standards-issuing country, actively promote the formation of regional and international IoT standardization bodies, win leadership positions on important international committees like ISO/IEC and ITU, and submit and respond to international proposals and motions, in order to increase China's international influence and competitiveness.[304]

Chinese state planners regard domestic IoT standardization work as a springboard for China's efforts to push its IoT standards in the international arena and understand the bureaucratic importance of holding key positions on international standards committees. The SPAPSF openly encourages experts in China's premier domestic IoT fields to take leadership positions, secretarial billets, and editing and convening roles in international technical standards organizations to

[298] Deutsches Institut für Normung (DIN, German Institute for Standardization), "China's Standardization Reform."

[299] "Standardization Law of the People's Republic of China (Full Text)," Standardization Administration of the People's Republic of China, January 2, 2018, http://202.99.59.128/sacen/law/201801/t20180102_340493.htm.

[300] "Standardization Law of the People's Republic of China (Full Text)."

[301] "国家标准委：正制定《中国标准 2035》" [National Standards Committee: "China Standards 2035" Is in Development], *中国新闻网 China News Network*, January 10, 2018, http://www.chinanews.com/gn/2018/01-10/8420700.shtml.

[302] [National Standards Committee: "China Standards 2035" Is in Development], *中国新闻网 China News Network.*

[303] "Special Project Action Plan for Internet of Things Development."

[304] Ibid., 8-9.

support standardization efforts led by China.[305] This is an explicit articulation of an implicitly understood bureaucratic reality: those who set the agenda and control the flow of paper in these international organizations stand a far greater chance of influencing ultimate outcomes in their favor.[306] Chinese officials view ownership of these sometimes thankless positions as an important part of China's efforts to dominate international standards.

Other important state plans for IoT-related technologies, like the 2017 New Generation Artificial Intelligence Development Plan illuminates the general Chinese strategy for influencing the global standardization of technological development, outlining seven main tasks designed to impact international AI development standards. These efforts closely parallel its strategy to become a leading IoT standardization tactics and include:[307]

- Encouraging domestic AI enterprises to "go out (走出去)," helping powerful AI enterprises conduct foreign mergers, providing stock investment, entrepreneurial investment, establishing foreign research centers;
- Encouraging foreign AI enterprises and research organizations to establish R&D centers inside China;
- Promoting establishment of international AI organizations and collectively formulating relevant international standards;
- Encouraging the use of AI in countries along the BRI through the creation of international AI cooperation bases and joint research centers
- Supporting relevant industry associations, alliances, and service organizations to build globalized service platforms aimed at AI enterprises;
- Encouraging AI enterprises to participate in or lead the development of international standards, using a technical standards "going out" approach to promote AI products and services in overseas applications.

Many of these methods are in active use in the IoT space and are described in detail below.

On High: Setting Formal Standards

An oft-quoted Chinese saying argues that "third-tier companies make products, second-tier companies make technology and first-tier companies make standards."[308] It is China's goal to become a first-tier power home to globally-leading companies, a goal it regards as intertwined with standards-setting. For this reason, China has moved to increase its influence in international standards-setting bodies using a variety of tactics, including coordinating lobbying efforts, seizing leadership opportunities, promoting Chinese experts, increasing contributions to the standards-formulation process, pushing for larger delegations and larger agendas.

[305] "Special Project Action Plan for Internet of Things Development," 10-11.

[306] One U.S. subject matter expert disagreed with this point, believing these billets alone do not provide sufficient authority to determine international technical standards. Chinese sources demonstrate that attaining these positions are part of a broader strategy to set agendas beneficial to China.

[307] State Council of the People's Republic of China, "新一代人工智能发展规划" (New Generation Artificial Intelligence Development Plan), July 8, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

[308] In Chinese: "三流企业做产品; 二流企业做技术; 一流企业做标准," as quoted in Breznitz and Murphree, "The Rise of China in Technology Standards."

China heralds acceptance of its preferred standards in these international bodies as national victories. In July 2018, *China Daily* reported that China's IoT Reference Architecture proposal submitted to the joint ISO/IEC body had passed the final draft international standard voting process. The standard, known as ISO/IEC 30141, was made by a research team from the Wuxi IoT Research Institute and will officially be published. *China Daily* described this development as a victory for the research team, which "against all odds…won the fierce international battle and sealed China's continuous leading position in the IoT industry."[309]

The result of this coordinated campaign is that Chinese participation in many cases rivals or outpaces the United States. The following table presents a brief summary of Chinese participation in major international standardization bodies with U.S. participation included for comparison, with a special focus on IoT-related standards entities. The subsequent sections offer more detail on Chinese tactics to raise and exert influence in these bodies.

[309] Zhou Wenbo, "ISO Chooses China's IoT Standards," *China Daily*, July 11, 2018, http://www.chinadaily.com.cn/m/jiangsu/wuxi/2018-07/11/content_36556927.htm.

Table 7: U.S. and Chinese Participation in International Standards Bodies

Organization	U.S. Participation Highlights	Chinese Participation Highlights
International Standardization Organization (ISO)	• Represented by the American National Standards Institute (ANSI) • One of 20 participating members on the ISO Council, the core governance body • Ranks 16th in technical committee participation • One of 25 participating member nations in ISO/IEC JTC 1/SC 41[310]	• Represented by the Standardization Administration of the People's Republic of China (SAC) • One of 20 participating members on the ISO Council, the core governance body • Ranks 4th in technical committee participation • One of 25 participating member nations in ISO/IEC JTC 1/SC 41[311]
International Electrotechnical Commission (IEC)	• Represented by the United States National Committee of the International Electrotechnical Commission (USNC/IEC), a totally integrated committee of ANSI[312] • Participating member in 169 technical committees and subcommittees, holds 26 secretariats[313]	• Represented by the Standardization Administration of the People's Republic of China (SAC) • Participating member in 181 technical and committees and subcommittees, holds 9 secretariats[314]
Internet Engineering Task Force (IETF)	• Steering committee members associated with U.S. companies like Google and nonprofits like IANA[315] • Formerly sponsored by the U.S. government	• Steering committee has a member associated with Huawei[316] • In 2013, the IETF chair toured China and noted the many Chinese IETF contributors, how China was

[310] "ISO/IEC JTC 1/SC 41: Structure," International Electrotechnical Commission (IEC), accessed September 4, 2018, http://iectest.iec.ch/dyn/www/f?p=103:29:7072304367374::::FSP_ORG_ID,FSP_LANG_ID:20486,25.

[311] "ISO/IEC JTC 1/SC 41: Structure," International Electrotechnical Commission (IEC).

[312] "United States National Committee of International Electrotechnical Commission (USNC/IEC), ANSI, accessed September 4, 2018, https://www.ansi.org/standards_activities/iec_programs/overview.

[313] "United States of America," International Electrotechnical Commission, accessed September 4, 2018.

[314] "China," International Electrotechnical Commission, accessed September 4, 2018, http://www.iec.ch/dyn/www/f?p=103:33:9703191523081::::FSP_ORG_ID,FSP_LANG_ID:1003,25; Ken Gettman, "Does China Deserve to Be an IEC Group A Member?" *Nema Currents* (blog), August 19, 2011, http://www.iec.ch/dyn/www/f?p=103:34:9703191523081::::FSP_ORG_ID,FSP_LANG_ID:1046,25.

[315] "IESG Members," Internet Engineering Task Force (IETF), accessed September 4, 2018, https://www.ietf.org/about/groups/iesg/members/.

[316] "IESG Members," Internet Engineering Task Force (IETF).

		second in authors after the United States, and the roles of Chinese contributors as working group chairs and Internet Architecture Board committee members, along with meeting hosts Tsinghua University and Huawei[317]
Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA)	• U.S. members of the IoT-specific IEEE Project 2413 include NIST, Cisco, Intel, IBM, Qualcomm	• Chinese members of the IoT-specific IEEE Project 2413 include Huawei and ZTE.[318] • Late 2017 news reports noted Huawei's success in submitting proposed smart city and edge computing standards for IoT at a P2413 work group meeting[319]
3GPP	• Represented by the Alliance for Telecommunications Industry Solutions (ATIS) • U.S. company representatives hold chair and vice-chair positions for 16/57 decision-making panels[320]	• Represented by the China Communications Standards Association (CCSA) • China is increasing its 3GPP presence while also investing heavily in the organization[321] • Chinese company representatives hold chair and vice-chair positions for 10/57 decision-making panels[322]
ITU Telecommunication	• 32 U.S. companies like Qualcomm, Symantec, Verizon, MediaTek, Lockheed Martin, Intel,	• Chinese national Zhao Houlin is Secretary-General

[317] Jari Arkko, "China," *IETF News*, September 19, 2013, https://www.ietf.org/blog/china/.

[318] "Internet of Things (IoT) Architecture Working Group," IEEE Standards Association, accessed July 23, 2018, http://grouper.ieee.org/groups/2413/member-list.html.

[319] Guy Daniels, "Huawei Doubles Down with Its Smart City Strategy," December 4, 2017, *TelecomTV,* https://www.telecomtv.com/content/smart-cities/huawei-double-down-with-its-smart-city-strategy-16214/; Daniel Golightly, "Huawei Helps Set Standards for Smart Cities & Edge Computing," *Android Headlines*, December 11, 2017, https://www.androidheadlines.com/2017/12/huawei-helps-set-standards-smart-cities-edge-computing.html.

[320] This count assumes that the representative from Motorola is Motorola Solutions, a U.S. company, and not Motorola Mobility, which is owned by Lenovo, a Chinese company. "Working Group Election Results," 3GPP, August 30, 2017, http://www.3gpp.org/news-events/3gpp-news/1896-wg_elections.

[321] Raymond Zhong, "China's Huawei Is at Center of Fight Over 5G's Future," *New York Times*, March 7, 2018, https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html; Stewart M. Patrick and Ashley Feng, "Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road," Council on Foreign Relations, July 2, 2018, https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road.

[322] "Working Group Election Results," 3GPP.

Standardization Sector (ITU-T)	Apple and AT&T participate in ITU-T as sector members[323] • NTIA is holds a vice-chair position at SG 20; the United States holds no rapporteur positions in any of the questions under study in the 2017-2020 period[324]	• 15 Chinese companies like Alibaba, China Mobile, China Unicom. Huawei, ZTE, China Unicom, China Telecom participate in ITU-T as sector members[325] • In SG 20, Fiberhome Tech Group, Wuhan University, ZTE, CAICT, Nokia Shanghai Bell, China Unicom, CETC Information Science Academy; in total, 2 out of 24 management team positions[326] and 9 out of 27 co- and associate rapporteur positions,[327] meaning every question under study has at least one Chinese representative

[323] "List of ITU-T Sector Members," International Telecommunications Union, accessed September 6, 2018, https://www.itu.int/online/mm/scripts/gensel11?_sect=T.

[324] "SG20: List of Questions and Rapporteurs (Study Period 2017-2020)," ITU-T, accessed July 23, 2018, https://www.itu.int/net4/ITU-T/lists/loqr.aspx?Group=20&Period=16.

[325] For a complete list, see "China," ITU-T, accessed May 23, 2018, https://www.itu.int/online/mm/scripts/gensel9?_ctryid=1000100502&_ctryname=China.

[326] "SG20 – Management Team (Study Period 2017-2020)," accessed September 6, 2018, https://www.itu.int/net4/ITU-T/lists/mgmt.aspx?Group=20. This includes one member with a listed affiliation with Nokia Solutions and Networks but an email address at "nokia-sbell.com," which is the domain for Nokia Shanghai Bell, a joint venture between Nokia and China Huaxin. The member herself is Dr. Xuan He. Aside from her email address, analysts did not find clear links to Nokia Shanghai Bell. Dr. He received a PhD from Beijing Institute of Technology and worked previously for the China Communications Standards Association, and appears to have a LinkedIn profile with a location set to Beijing. For more information, see. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/iot/20151019/Pages/HE-Shane.aspx and https://cn.linkedin.com/in/shane-he-82965968.

[327] "SG20: List of Questions and Rapporteurs (Study Period 2017-2020)," ITU-T, accessed July 23, 2018, https://www.itu.int/net4/ITU-T/lists/loqr.aspx?Group=20&Period=16.

Coordinated Lobbying Efforts

Part of the effort to push for Chinese standards internationally involves coordinating domestic players to advocate for the same priorities abroad. To this end, China established the IMT-2020 5G Promotion Group in 2013 to coordinate efforts by mobile service operators, manufacturers and research institutes. The group is a cooperative effort between three Chinese ministries (the MIIT, NDRC, and MOST),[328] and is not only charged with promoting 5G research domestically but also with facilitating international communication and cooperation.[329] The group notes that it "is willing to strengthen cooperation with global organizations, enterprises, universities, and research institutes to jointly define the 5G concept and technology roadmap, and work together to promote globally unified 5G standardization and industrialization."[330] The companies and organizations involved in the IMT-2020 (5G) Promotion Group include China Mobile, China Telecom, China Unicom, Huawei, ZTE, the Datang Telecom Technology & Industry Group, Beijing University of Posts and Telecommunications, and Tsinghua University.[331] Beyond coordinating domestic Chinese entities, the IMT-2020 (5G) Promotion Group has also been active in ensuring cooperation with international standards organizations. Its organizational structure highlights working groups for the ITU, 3GPP, and IEEE specifically, alongside a general international cooperation working group.[332] On June 3, 2016, IMT-2020 (5G) Promotion Group and the international standard body 5GPPP announced the signing of a memorandum of understanding that promotes "comprehensive and in-depth cooperation in 5G, but also lays a foundation to facilitate globally unified 5G standardization as well as the development of 5G industry and applications."[333]

Chinese companies also face pressure to vote together in international organizations. When Lenovo initially voted against a proposed Huawei standard in a first-round 3GPP vote by backing what it believed to be a superior standard and one more in line with its IP holdings, it faced such public outcry and criticism in Chinese media that the company's founder released an apologetic statement emphasizing that "We all agree that Chinese companies should be united and cannot be

[328] "组织架构" [Organization Framework], IMT-2020 (5G) Promotion Group IMT-2020 (5G) 推进组, accessed April 17, 2018, http://www.imt-2020.org.cn/zh/category/65588.

[329] IMT-2020 (5G) Promotion Group, "White Paper on 5G Concept," accessed May 23, 2018, http://webcache.googleusercontent.com/search?q=cache:TDbcMTJ1OaIJ:www.imt-2020.org.cn/en/documents/download/3+&cd=6&hl=en&ct=clnk&gl=de.

[330] IMT-2020 (5G) Promotion Group, "White Paper on 5G Concept."

[331] "5G Progress and Cooperation in China," China Academy of Information and Communications Technology, April 2016, http://www.chinaeu.eu/wp-content/uploads/2016/04/mazhigang-5G-Progress-and-Cooperation-in-China-20160408.pdf. In February 2018, the U.S. firm Keysight Technologies claimed to have become the first and only international test and measurement company to be a full member of the IMT-2020 (5G) promotion group, a body that appears to otherwise have exclusively Chinese participants and proclaims itself the major platform to promote research on 5G in China. See: "Keysight Technologies Announces Formal Membership in China IMT-2020 (5G) Promotion Group," *Keysight Technologies,* February 12, 2018, https://about.keysight.com/en/newsroom/pr/2018/12feb-nr18005.shtml.

[332] "5G Progress and Cooperation in China" (slide presentation), CAICT, April 2016, http://www.chinaeu.eu/wp-content/uploads/2016/04/mazhigang-5G-Progress-and-Cooperation-in-China-20160408.pdf.

[333] "IMT-2020 (5G) Promotion Group and 5G PPP Announce Memorandum of Understanding for 5G," IMT-2020 (5G) Promotion Group, June 3, 2016, accessed May 23, 2018, http://www.imt-2020.org.cn/en/news/detail/22.

played off one another by outsiders."[334] This indicates that private companies in China are likely to band together in standards votes to avoid criticism of anti-China behavior.

Seizing Leadership Opportunities

China has increasingly pushed for larger roles in standards-setting bodies, both for government representatives and for Chinese companies. According to Edison Lee and Timothy Chau, analysts at the U.S. investment bank Jeffries (Hong Kong), this is especially apparent in the ITU, a key standards-setting body within the UN system where Chinese government-backed think tanks and corporations hold a multitude of leadership roles in focus and working groups, and 3GPP, where China, primarily through Huawei and China Mobile, has "aggressively sought leadership positions" in order to raise its influence.[335] Within 3GPP, Huawei holds multiple senior leadership positions, including six vice chairmanships and two full chairmanships in various sub-committees and working groups.[336] This presence is neither an accident nor merely a simple reflection of the size of Chinese telecoms, but rather the result of a deliberate effort to place experienced Chinese technical experts in positions of influence in critical international standards bodies. This tracks with Chinese efforts to steer its way to a larger influence in the UN by first taking leadership of previously-undesirable or lower-impact committees and using them to promote Beijing's interests through a combination of holding the top leadership slots and contributing funding.[337]

Chinese experts are also seizing leadership opportunities in other international standards bodies, which could lead to more opportunities to control agendas and priorities. Since taking its first responsibilities in international work teams in 2004 within the International Organization for Standardization (ISO), China's presence had skyrocketed to include the heads of more than 30 committees and sub-committees by 2012. The Chinese government's strategy is in many cases to overwhelm the system with requests: as the former head of French national standards body AFNOR and vice-president of finance for ISO put it, "As soon as a chair is vacant, Beijing submits an application."[338] As of 2018, China held the secretariat position in 61 technical committees (TCs), was a twinned secretariat in 17 TCs, a participating member in 683, and an observing member in 50, tying for the third-highest country in technical committee participation (See Table 4).[339]

Within 3GPP, Huawei is the chair of the SA2–Architecture working group,[340] the body looking at the second "standalone" phase of 5G (where China hopes to dominate). Huawei also holds the vice

[334] In Chinese: "我们一致认为，中国企业应团结，不能被外人所挑拨。" Liu Chuanzhi, Yang Yuanqing, and Zhu Linan, "行动起来，誓死打赢联想荣誉保卫战！" [To Arms, Win the Defensive Battle for Lenovo's Honor!], Weixin.QQ.com, May 16, 2018, https://mp.weixin.qq.com/s/JDlmQbGFkxu-_D2jsqNz3w.

[335] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," Jeffries LLC, September 14, 2017, https://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf.

[336] "Radio Communication Standards," Huawei 华为, accessed May 23, 2018, http://www.huawei.com/us/industry/standards-contributions/hw-u_167829.htm##.

[337] Colum Lynch, "China Enlists U.N. to Promote Its Belt and Road Project," *Foreign Policy,* May 10, 2018, https://foreignpolicy.com/2018/05/10/china-enlists-u-n-to-promote-its-belt-and-road-project/.

[338] Olivier Peyrat, "China's Standardization Strategies," *Paris Innovation Review,* October 9, 2012, http://parisinnovationreview.com/articles-en/chinas-standardization-strategies.

[339] "SAC: China," International Standards Organization, accessed September 5, 2018, https://www.iso.org/member/1635.html.

[340] "3GPP Officials for Group: 3GPP SA 2 ("S2")," 3GPP, accessed May 17, 2018, http://www.3gpp.org/DynaReport/TSG-WG--S2--officials.htm.

chair position in the SA5–Telecom Management working group.[341] Similarly, ZTE has been "advancing its leadership in global and domestic SDOs [standards developing organization] arena," with leadership positions at IEEE, the WPAN working group under China NIST, 3GPP, ETSI Multi-access Edge Computing Industry Specification Group projects, and on the board of the OpenFog Consortium.[342]

China has also seized leadership opportunities in groups it has proposed creating, like a new ISO research group on the integration of the IoT and blockchain. *Science and Technology Daily*, the official MOST newspaper, declared the creation of the group an indication that China has won "discursive power" (话语权) in the development of next-generation information technology integration and innovation.[343] Proposing new groups has also allowed Chinese chairs to lead the group, as is the case for the new IoT and blockchain group, which will be chaired by Dr. Shen Jie, who is head of the China Internet of Things Basic Standards Working Group.

Zhao Houlin

China has increased its representation at the top levels of leadership of these bodies. For example, ITU's current secretary-general is Chinese national Zhao Houlin,[344] who formerly worked in China's Ministry of Posts and Telecommunications and was active in expert meetings on telecommunications standards meetings and national plans.[345] While ostensibly a neutral global bureaucrat, Zhao's past statements and the view Chinese sources take of his work suggest that both he and the PRC view him as an agent of Chinese interests.

Zhao often adopts a neutral, consensus-oriented outlook in public statements to English-language media, his Chinese-language statements reveal a focus on promoting Chinese interests.[346] A biography of Zhao described his deep feelings that his work at the ITU and the development of his "motherland's" ICT industry are closely linked.[347]

Zhao Houlin's work has been portrayed through a nationalist lens in Chinese media reports. One noted that he "uses strength to fight for China's right to speak" and that "within the scope of Zhao Houlin, China's self-developed TD-SCDMA and TD-LTE have become one of the major technical

[341] "3GPP Officials for Group: 3GPP SA 5 ("S5")," 3GPP, accessed May 17, 2018, http://www.3gpp.org/DynaReport/TSG-WG--S5--officials.htm.

[342] "ZTE Designated as the Chair of Newly Formed IEEE802.11 NGV SG," ZTE (press release), April 13, 2018, http://www.zte.com.cn/global/about/press-center/news/2018-Ma-April/April-13.

[343] Guo Guozhong 过国忠, "中国主导国际物联网与区块链融合标准研究" [China Leads International Internet of Things and Blockchain Integration Standards Research], *科技日报 Science and Technology Daily*, July 18, 2018, http://www.stdaily.com/guoji/luntan/2018-07/18/content_690980.shtml.

[344] Zhao Houlin, "How ITU Helps to Create a New Mobile Era via 5G," ITU News, February 28, 2018, http://news.itu.int/itu-helps-create-new-mobile-era-via-5g/

[345] "Biography: Houlin Zhao," International Telecommunications Union, accessed May 23, 2018, https://www.itu.int/en/osg/Pages/biography-zhao.aspx.

[346] "国际电联全权代表大会召开扬州人赵厚麟：秘书长唯一候选人" ["ITU Plenipotentiary Conference Opens, Yangzhou Native Zhao Houlin Sole Candidate for Secretary-General"], October 23, 2014, http://news.yzwb.com/system/2014/10/23/010764066.shtml.

[347] "Zhao Houlin," China Mobile Labs, September 28, 2010, https://web.archive.org/web/20110912045947/http://labs.chinamobile.com/innobase/i-4409.html.

standards recommended by the ITU for 3G and 4G respectively."[348] Others referenced instances when his support for developing nations served Chinese interests, like his support for Chinese-developed TD-SCDMA and TD-LTE as global standards,[349] helping China avoid paying royalties to use alternative proprietary standards.

Zhao often reflects the Chinese view that U.S. management of key internet governance institutions is undesirable. When asked whether the U.S. government's involvement in ICANN is a problem, Zhao responded, "to some extent, yes. That is why people are raising this issue as a very important one to be debated at the UN and in the (World Summit) process. Some people have argued very strongly that ICANN's establishment based in California gives people some worries. This issue should be addressed."[350] He further argued that "people realize today that governments worldwide have to play a role," language that mirrors arguments other authoritarian states have made in seeking to carve out a greater role for the ITU and individual nation-states in setting internet policy. Indeed, Zhao has also argued that the "ITU must be positioned as the United Nations' preeminent technical agency for worldwide cooperation in terms of spectrum harmoni[z]ation, global ICT standards that benefit the whole sector, and capacity building and knowledge sharing in every region."[351]

Beyond his work at the ITU, Zhao is an honorary dean of the NUPT School of Communication and Information Engineering.[352] Chinese media has noted that "in recent years, Zhao has often returned to his alma mater to introduce cutting-edge technology and current trends in the field of international communication and information."[353] This reportedly includes areas of future ITU emphasis, giving NUPT and affiliated institutions a potential advantage in starting relevant research (and potentially commercialization) programs early. Other articles reporting his loyalty to NUPT quote him as saying, "As long as it is good for my alma mater, I am willing to do it," a loyalty that doubles as a stand-in for his allegiance greater Chinese good.

Promoting Chinese Experts

China has also been working to put forward its own experts internationally in discussions of key technologies. These experts in turn, once elevated to the international stage, continue to be involved in and promote national standards-setting efforts both during and after their tenures (as with Zhao Houlin at the ITU). Zhang Xiaogang, the former chairman of the ISO, attended the kick-

[348] "南邮大教授赵厚麟当选电联秘书长" ["NUPT Professor Zhao Houlin Elected as Secretary-General of the ITU"], 扬子晚报-扬网 [Yangzi Evening News Online], October 24, 2014, http://pic.yangtse.com/epaper/yaowen/2014-10-24/326482.html.

[349] "Zhao Houlin," The 4th TD-LTE Technology and Spectrum Workshop (speech transcript), December 18, 2014, http://www.gtigroup.org/2014doha/speaker/2014-11-20/4910.html.

[350] Declan McCullagh, "The U.N. Thinks about Tomorrow's Cyberspace," *CNet*, March 29, 2005, https://www.cnet.com/news/the-u-n-thinks-about-tomorrows-cyberspace/.

[351] "ITU's New Head Plans to Connect Technology Parks to Share Experiences in Emerging Markets" interview with Houlin Zhao, *Global Telecoms Business* No. 137 (November-December 2014): 28-29, http://about.att.com/content/dam/snrdocs/global_telecomms_business_nov_dec_2014.pdf.

[352] "我校杰出校友、国际电信联盟秘书长赵厚麟会见多国政要" ["Our Outstanding Alumnus and Secretary-General of the International Telecommunications Union, Zhao Houlin, Met with Political Figures from Many Countries"], Nanjing University of Posts and Telecommunications, September 22, 2017, http://www.njupt.edu.cn/2017/0919/c53a113277/page.htm.

[353] ["NUPT Professor Zhao Houlin Elected as Secretary-General of the ITU"], [Yangzi Evening News Online].

off meeting (for Standards 2035), a national plan aiming to increase Chinese standardization internationally, among other goals.[354]

In numeric terms, Chinese expert participation in key international standards bodies has increased dramatically in the past twenty years. A NIST review of IEC expert participation by country found that in 2005, China was not among the top ten, but by 2012 it had jumped to fifth place.[355] While a more updated review is not available, it is likely that Chinese expert participation has continued to grow in the intervening years.

China has also been taking a larger role in hosting events that feature its experts. In April 2018, the China Academy of Information and Communications Technology (CAICT), a MIIT think tank that plays a role in policy and standards development, collaborated with ITU to present a workshop on the "Impact of AI on ICT Infrastructures."[356] The workshop was hosted by the Xi'an high tech district government, and co-hosted by China Mobile, China Unicom, and China Telecom.[357] The workshop took place at a ZTE hotel as part of the Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G). Among the speakers were representatives from MIIT, CAICT, 21Vianet, Alibaba, Huawei, Baidu, China Unicom, China Mobile, China Telecom, Xi'an Jiaotong University, and the State Key Lab for the Management and Control of Complex Systems within the Institute of Automation at the Chinese Academy of Science.[358] Several of the represented organizations Chinese government organizations or otherwise have close ties to China's strategic effort for dominance of IoT standards.

Increasing Contributions

U.S. company Qualcomm has complained about "contribution counting" in 3GPP, the practice of dividing contributions into as many different documents as possible so as to appear to be responsible for a greater portion of the technical contributions and investments in the standard setting process, allowing members to seek IPR through the IPR policies of regional standards setting organizations that partner with 3GPP.[359] While Qualcomm does not name any members in particular, China is fond of citing the number of contributions it has made to 3GPP, and others have noted that "Chinese submissions are ubiquitous" in 3GPP working groups.[360] As of early 2017, Huawei had submitted 234 contributions to 3GPP, the most of any member.[361] The ubiquity of its contributions allows China to take advantage of the standards system's tendency toward compromise to earn acceptance for a portion of its proposals. This was in evidence in the

[354] "'中国标准 2035'项目在京启动" ["'China Standards 2035' Project Started in Beijing"] *中国质量报* [*China Quality News*], March 2, 2018, http://www.aqsiq.gov.cn/zjxw/zjxw/zjftpxw/201803/t20180302_513610.htm.

[355] Choi and Puksar, "NISTIR 8007."

[356] "Impact of AI on ICT Infrastructures," ITU workshop, Xi'an, China, April 25, 2018, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180425/Pages/default.aspx.

[357] "Impact of AI on ICT Infrastructures," ITU workshop, Xi'an, China, April 25, 2018, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180425/Pages/default.aspx.

[358] "Programme: Impact of AI on ICT Infrastructures," ITU workshop, Xi'an, China, April 25, 2018, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180425/Pages/programme.aspx.

[359] "Top 5 Drawbacks of 'Contribution Counting' in 3GPP. (Don't Count on It!)," *OnQ Blog*, Qualcomm, August 2, 2017, https://www.qualcomm.com/news/onq/2017/08/02/top-5-drawbacks-contribution-counting-3gpp-dont-count-it.

[360] Burstein, "China: We Lead 3GPP Wireless Standards."

[361] Newley Purnell and Stu Woo, "China's Huawei Is Determined to Lead the Way on 5G Despite U.S. Concerns," *Wall Street Journal,* March 30, 2018, https://www.wsj.com/articles/washington-woes-aside-huawei-is-determined-to-lead-the-way-on-5g-1522402201.

acceptance of Huawei's Polar code error-control technique in a key 3GPP standard for 5G, discussed in more detail in the 5G case study below.

Larger Delegations and Larger Agendas

Alongside the high number of proposed contributions China is making in international standards organizations, China tends to bring large delegations to meetings, which may give it the added capacity to consider a larger number of issues at any given meeting. China's desire to increase the number of topics under consideration at international conferences has led to friction with companies like Ericsson, which wanted to consider a smaller number of issues. In an interview, Ericsson's head of standardization pointed to the company's smaller delegation and the onerous workload of the conferences, saying "We do not intend to flood the process,"[362] a pointed contrast with the Chinese approach. The eventual compromise took China's wishes into account and settled at a middle number.

On the Ground: Setting De Facto Standards

In globalized technology standards, there is an inherent advantage to whomever can research and develop a new technology and patent its components first. China's extensive state funding for expedited R&D on communications technologies targets this goal, an investment that is already yielding results in the IoT and its attendant technologies. This support has translated into greater influence in international standard-setting. By providing a practical roadmap of how new technologies can be adopted at scale, China can shape debates over how those standards should be implemented worldwide. The PRC's approach varies depending on the specific technology in question, but the strategy generally includes three basic tenets:

- The PRC government supports testing of a new technology at a local level (generally through a single municipality), and gradually begins to deploy it at scale both domestically and abroad using state plans, extensive direct government funding, and massive subsidies to "national champion" companies.[363]
- Offices within the government draw up a series of standards governing the use of targeted technology within the PRC.
- Chinese negotiators are able to take the practical example of a technology's use and the standards governing it as a kind of "pre-built" model for the technology's implementation, enabling them to box out challenges from other standards models.

These measures establish a self-reinforcing cycle in which initial deployment of technology aids favorable international standardization efforts, which in turn aid deployment at scale.

Financing Accelerated R&D Development

As one of its many means for expediting research progress, China has invested heavily in the IoT, establishing a multi-million-dollar IoT fund.[364] On 5G, estimates predict that China will surpass

[362] At this particular conference (where conflict with Ericsson and Huawei was reported), Samsung had 41 representatives, Huawei had 40, Qualcomm had 30, Ericsson had 25, and Nokia had 18. See Purnell and Woo, "China's Huawei Is Determined to Lead."

[363] Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental, February 2017, https://new.reorg-research.com/data/documents/20170928/59ccf7de70c2f.pdf.

[364] "What's at Stake in China's 5G Push?" *APCO Forum*.

$443 billion in total network investment from 2020-2030, more than the cost of any other telecommunications infrastructure constructed on the mainland.[365] Much of that investment will come from the big three state telecommunications companies, which CAICT estimates will hit $47 billion in 2023.[366]

Much of this support goes to designated "national champions" in a push to ensure that Chinese firms become competitive globally. Chinese government support for these companies can be hard to quantify, but it is suspected to range from outright subsidies for government-desired tech objectives to favorable loan financing and other encouraging policy measures. This investment allows Chinese companies to position themselves favorably in designing and patenting the backbone technologies necessary new global telecommunications electronics and infrastructure.

Growth in international patent and trademark filings comes primarily from Chinese company filings, according to the director general of the World Intellectual Property Organization.[367] This is evident in the patent filings of Huawei and ZTE, two of China's "national champions." In 2016, ZTE ranked first in the WIPO list of annual patent applications. The company reported that the 4,123 patent filings are driven by R&D on next-gen technologies like 5G, IoT, cloud computing, big data, and smart city.[368] Huawei followed closely behind, ranking second with 3,692 patent applications, ahead of Qualcomm (2,466) and Mitsubishi (2,053).[369]

Chinese firms are already stockpiling advantages that will pay off in ongoing and future competitions over standardization. In the fight for 5G, Huawei and ZTE own some 10 percent of 1,450 5G patents compared to Qualcomm's 15 percent, Nokia's 11 percent, and Ericsson's 8 percent.[370] Huawei and ZTE's holdings include standard-essential patents (SEPs) that will generate royalty payments from other companies making products in the field.[371] Holding an edge in the number of SEPs would entitle Chinese companies like Huawei and ZTE to receive significant royalty payments and potentially undermine the ability of U.S. firms to innovate and compete, a mechanism cited by CFIUS in its 2018 rejection of the Broadcom attempt to acquire

[365] Li Tao, Yingzhi Yang, and Bien Perez, "China's 5G Expansion Plans Threatened as ZTE is Pinched by US Export Ban, Trade Tensions," *South China Morning Post*, April 17, 2018, http://www.scmp.com/tech/social-gadgets/article/2142154/chinas-5g-expansion-plans-threatened-zte-export-ban-trade; Bien Perez, Sarah Dai, and Catherine Wong, "Trump's Rush to Build a National 5G Network May Backfire, Give China the Technological Edge," *South China Morning Post*, January 29, 2018, http://www.scmp.com/tech/enterprises/article/2131082/us-5g-nationalisation-plan-seen-reflecting-mistrust-may-hand-china.

[366] Luigi Gambardella, "China Is Set to Lead in Global 5G Race," *China Watch*, July 19, 2018, http://www.chinawatch.cn/a/201807/19/WS5b502176a31083ed8f129aba_1.html.

[367] "ZTE Moves to No. 1 in World Intellectual Property Organization's Patent Table," Cision PR Newswire (press release), March 16, 2017, https://www.prnewswire.com/news-releases/zte-moves-to-no-1-in-world-intellectual-property-organizations-patent-table-300424644.html.

[368] "ZTE Moves to No. 1 in World Intellectual Property Organization's Patent Table," Cision PR Newswire.

[369] "Record Year for International Patent Applications in 2016; Strong Demand Also for Trademark and Industrial Design Protection," WIPO, March 15, 2017, http://www.wipo.int/pressroom/en/articles/2017/article_0002.html.

[370] Raymond Zhong, "China's Huawei is at Center of Fight over 5G's Future," *New York Times*, March 7, 2018, https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html.

[371] A July 2018 estimate of companies' actual 5G standards-essential patent (SEP) portfolios (an adjustment intended to correct for flaws in companies' self-reported SEP holdings) predicted that Qualcomm holds 8.6% of patents, followed by Huawei at 7.92%, LG with 7.38%, Ericsson with 6.74%, Samsung with 5.77%, and ZTE with 4.1%. See: Tim Pohlmann "Industry Report: Who Will Be the Technology Leader for 5G? Part Two," I Am Media and IPlytics, July 18, 2018, https://www.iam-media.com/who-will-be-technology-leader-5g-part-two.

Qualcomm.[372] Owning these 5G patents also helps Chinese firms submit more cost-effective bids for 5G network projects, increasing their market share, and strengthening their hand in standardization competition.

China's domestic and foreign policies also ensure market share for its leading 5G developers and providers, building up leverage for future standardization competition. Chinese policy guarantees Huawei and ZTE each approximately one-third of China's 5G network contracts, leaving foreign firms like Nokia and Ericsson to compete for much smaller slices.[373] There are signs that these measures are paying off. China has rolled out various component technologies ahead of its competitors in the hopes that a working prototype will lend weight to its preferred standards. At the 2018 Mobile World Congress in Barcelona, China Mobile announced the "world's first 5G CPE (customer premises equipment) based on 3GPP standard[s]," manufactured by Huawei Technologies. The CPE box runs on the preferred Chinese low frequency band at 3.5GHz,[374] rather than the U.S.-backed mmWave frequency band, highlighting an area of contention where China aims to pair a first-mover advantage with centralized support for its standards agenda.

"Going Out" and Establishing a Global Commercial and Industry Footprint

Both individual Chinese companies and broader government-sponsored alliances are acting in clear alignment with government directives to "go out" to promote Chinese technology abroad. Some of this global footprint is directly relevant to international standards, while other elements of China's global IoT and 5G presence indirectly contribute to China's international standardization ambitions by increasing China's commercial clout in multiple locations overseas. Establishing a global footprint for China's IoT and 5G "national champions" is a major component of China's international standardization effort.

ZTE is an example of a Chinese company that has followed this "going out" directive and increased its influence abroad through international research centers, strategic partnership agreements with foreign multinational companies, work to formulate international standards in existing standards organizations, and founding its own global alliances. For example, ZTE operates 20 R&D centers in Asia, North America, Africa, the Middle East, and Europe.[375] To increase its market share in Europe, the company has also pursued bilateral agreements with multinational telecommunications operators. In 2016, ZTE signed a memorandum of understanding with Telefonica, the Spanish broadband and telecommunications provider, for development of 5G technologies.[376] In 2017, it announced a strategic partnership agreement with Belgium's Telenet to collaborate on 5G and IoT.[377] ZTE has also followed the directive to promote the establishment

[372] Aimen N. Nir, "Letter Re: CFIUS Case 18-036: Broadcom Limited (Singapore)/Qualcomm Incorporated," United States Department of the Treasury, March 5, 2018, https://www.qcomvalue.com/wp-content/uploads/2018/03/Letter-from-Treasury-Department-to-Broadcom-and-Qualcomm-regarding-CFIUS.pdf.

[373] Eric Auchard and Sijia Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks," Reuters, 23 February 23, 2018, https://www.reuters.com/article/us-telecoms-5gchina/chinas-huawei-set-to-lead-global-charge-to-5g-networks-idUSKCN1G70MV.

[374] Dan Jones, "China Mobile Claims First 3GPP Standard 5G CPE," *Light Reading 5G*, February 27, 2018, https://www.lightreading.com/mobile/5g/china-mobile-claims-first-3gpp-standard-5g-cpe/d/d-id/740908.

[375] "ZTE Opens New R&D Center in Japan to Boost 5G Research," ZTE Corporation (press release), November 4, 2015, http://www.zte.com.cn/global/about/press-center/news/201511/445626.

[376] "ZTE and Telefonica Partner on 5G," ZTE Corporation (press release), June 23, 2016, http://www.zte.com.cn/global/about/press-center/news/2016623ma/2016623ma.

[377] "ZTE Signs Strategic Partnership with Telenet on 5G and IoT," ZTE Corporation (press release), June 2, 2017, http://www.yslxgy.com/global/about/press-center/news/201706ma/0605ma2.

of international organizations by founding the Global IoT Alliance, which it claims to have "more than 200 partners from more than 30 industries."[378]

The company has also followed the directive to participate in international standardization activities. As a self-proclaimed "major participant and contributor to global 5G technologies and standards," ZTE is a member of more than 70 standards organizations, alliances, and forums. This includes major international bodies like the ITU, 3GPP, and IEEE, as well as China's domestic IMT-2020 (5G) Promotion Group.[379] The company is a member of specialized sub-IoT associations, like the 5G Automobile Association (5GAA), a cross-industry alliance that will allow ZTE to "team up with industrial partners to further promote the smart Internet of Vehicles."[380] It claims to be an active participant and leader in the MEC standardization process in the European Telecommunications Standards Institute (ETSI) and 3GPP and notes that with its "powerful R&D capability," the company has developed its own MEC solution,[381] another example of leveraging R&D advances to lead standardization efforts.

Other Chinese "national champions" are equally active in establishing a global presence. In addition to its participation in major standards bodies, Huawei has also set up research centers abroad.[382] For instance, Huawei's chief executive has singled out Italy as particularly "fertile ground" for cooperation and investment. The company has set up three centers in collaboration with Telecom Italia and a Core Network Innovation Center with Vodafone. The company notes explicitly what it hopes to gain from this cooperation:

> Huawei, which has been present in Italy for the past 13 years, is actively looking to partner with Italian companies in 'Industry 4.0', the 'internet of things', smart cities, and all other areas where its key technologies can be used. In the longer term, Huawei hopes to become a bridge in Sino-Italian and Sino-European cooperation. In the 5G sector, for example, it hopes to be part of the discussion for shaping global norms and standards alongside the EU.[383]

For its part, China Mobile aims to expand international partnerships through cooperation with the Global TD-LTE Initiative (GTI), which was founded to promote China's preferred 4G TD LTE

[378] "ZTE Joins 5GAA," ZTE Corporation (press release), January 9, 2017, www.zte.com.cn/global/about/press-center/news/201701ma/0109+&cd=1&hl=en&ct=clnk&gl=de. See also "ZTE's NB-IoT Innovative Application Wins GLOMO Award at MWC2018," Cision, February 26, 2018, https://www.newswire.ca/news-releases/ztes-nb-iot-innovative-application-wins-glomo-award-at-mwc2018-675232973.html.

[379] "ZTE Signs Strategic Partnership with Telenet on 5G and IoT."

[380] "ZTE Joins 5GAA," ZTE Corporation (press release).

[381] "ZTE and China Unicom Demonstrate 5G MEC-based VR Service Solution," ZTE Corporation (press release), June 29, 2016, http://www.zte.com.cn/global/about/press-center/news/2016629ma3/2016629ma3.

[382] Huawei also has facilities in the United States, including R&D facilities in Santa Clara, California, and Bridgewater, New Jersey. See "Facts and Figures," Huawei USA, accessed September 6, 2018, http://usahuawei.com/who-we-are/facts-and-figures/.

[383] 5G spectrum in Europe is determined at the national level, despite EU efforts at coordination. See Mark Scott, "Mobile World Congress to Show Why Europe is the World's 5G Laggard," *Politico*, February 26, 2018, https://www.politico.eu/article/mobile-world-congress-mwc-5g-europe-china-us-telecommunications-network/. Jérôme Doyon & François Godement, "China and the Mediterranean: Open for Business?" European Council on Foreign Relations, June 21, 2017, http://www.ecfr.eu/publications/summary/china_and_the_mediterranean_open_for_business.

standard; the GSMA, an originally-European mobile industry group; the Next Generation Mobile Networks Alliance (NGMN); and other international organizations.[384]

China's global IoT and 5G presence has also spread to the United States. Chinese companies have found success selling to lower-tier telecommunications carriers in the rural United States, often by offering lower prices than other U.S. or international competitors.[385] Sagebrush Cellular, SpeedConnect, Union Wireless and United Wireless are four such Tier 3 carriers.[386] The Rural Wireless Association, an industry group for U.S. telecommunications companies with fewer than 100,000 subscribers, has even elected a Huawei executive to its board, the only representative not from a U.S. telecommunications company.[387] Their general counsel noted that "these carriers love Huawei gear" and that they are reliant on Huawei support.[388] Huawei's presence is an indicator of its determination to gain a foothold in the United States, even through smaller, rural carriers, a strategy it has used with success.

Wooing Allies

Emerging Markets: The Belt and Road Initiative

China has linked Xi Jinping's signature economic and foreign policy initiative, the Belt and Road Initiative (BRI), to building infrastructure in developing nations in an effort to forestall a slowing of the Chinese economy while also increasing China's influence around the world. In signing contracts to build high-speed rail and telecommunications systems, China will also be able to convert these nations to use its proprietary technologies. The strategy of using the BRI to export Chinese technological and engineering standards makes for what the Lowy Institute termed "one of the least understood aspects" of the initiative.[389] In keeping with Xi Jinping's directives, the SAC has vowed to "promote the application of Chinese standards in the course of developing the Belt and Road Initiative."[390]

A substantial proportion of BRI investments will be in the information and communications technologies (ICT) sector. These prospects are not lost on Chinese leaders in international standards bodies, who have emphasized that ICT investment is a critical part of BRI.[391] This moves

[384] "ZTE Proud to Be Launch Partner in China Mobile's 5G Joint Innovation Lab (JIL)," ZTE Corporation (press release), February 26, 2018, http://www.zte.com.cn/global/about/press-center/news/201602/201602265GUnion.

[385] Phil Goldstein, "Huawei Exec: We Treat Tier 3 U.S. Carriers Like They're the 'Belle of the Ball,'" *FierceWireless*, March 27, 2015, https://www.fiercewireless.com/wireless/huawei-exec-we-treat-tier-3-u-s-carriers-like-they-re-belle-ball.

[386] Goldstein, "Huawei Exec: We Treat Tier 3 U.S. Carriers Like They're the 'Belle of the Ball.'"

[387] "Board of Directors," Rural Wireless Association, accessed September 6, 2018, https://ruralwireless.org/about-rwa/.

[388] Raymond Zhong, Paul Mozur, and Jack Nicas, "Huawei and ZTE Hit Hard as U.S. Moves against Chinese Tech Firms," *New York Times*, April 17, 2018, https://www.nytimes.com/2018/04/17/technology/huawei-trade-war.html.

[389] Peter Cai, "Understanding China's Belt and Road Initiative," Lowy Institute for International Policy, March 2017, https://www.lowyinstitute.org/sites/default/files/documents/Understanding%20China%E2%80%99s%20Belt%20and%20Road%20Initiative_WEB_1.pdf.

[390] "Action Plan on Standards to Build the Belt and Road Initiative," Standardization Administration of the People's Republic of China, March 27, 2018, http://202.99.59.128/sacen/Features/201803/t20180327_342070.htm.

[391] Houlin Zhao, "China's One Belt, One Road Can Improve Lives at Scale through ICT Investment," *ITU News*, May 16, 2017, http://news.itu.int/chinas-one-belt-one-road-can-improve-lives-at-scale-through-ict-investment.

into a part of the initiative dubbed the "Digital Silk Road" (数字丝绸之路).[392] These overseas ICT investments will provide China with leverage over developing countries to influence international technical standards bodies like the ITU as BRI projects build out infrastructure to PRC technical standards.

China's "national champions" have been an active part of this effort. The favorable treatment they enjoy from the Chinese government guarantees that the companies can compete and win internationally. Firms without such government backing have difficulty going up against Chinese champions, who often underbid them. ZTE has been accused of unfair practices, including pricing under cost.[393] One such area where the support of the Chinese government proves key is in bidding for market share in developing nations. As a 2017 DoD-commissioned report notes, in competitions for emerging market business in parts of the world like Africa:

> The Chinese government joins Huawei and brings a portfolio of additional offerings to bear on a deal. For example, the Chinese government might offer to build infrastructure in an emerging market, finance this with low-cost capital from the China Development Bank and, in the process, provide jobs in the community in addition to supporting Huawei with subsidies for extremely competitive pricing on telecommunications and networking gear.[394]

This has the dual advantage of extending Huawei's market share and increasing the Chinese government's influence in these nations, many of whom go on to support Chinese positions in intergovernmental bodies.

The ultimate impact of China's increasing global commercial presence is unclear but increasingly points toward pushing an agenda favorable to authoritarian regimes. One prominent example suggesting that Beijing had used its leverage to influence international standards organizations occurred in 2012, when members of the ITU met to review proposed revisions the International Telecommunication Regulations (ITR), a legally binding international treaty governing the internet. China and Russia, in partnership with many developing countries and repressive states like Saudi Arabia, Sudan, and Egypt, put forward a proposal to rephrase the treaty to enshrine greater national sovereignty over the internet, re-defining the global internet as an "international conglomeration of interconnected telecommunication networks" with internet governance falling to member states, who would retain sovereign rights to implement related policies.[395] A second group of countries led by the United States, however, defended "the open internet" and refused to

[392] "China Needs to Develop e-Commerce, Industrial Networks, Internet Banking: Ren," State Council of the People's Republic of China (from *China Daily*), July 17, 2015, http://english.gov.cn/news/top_news/2015/07/17/content_281475148857772.htm.

[393] Jeremy Horwitz, "ZTE Chases 5G Growth in Japan as U.S. Shuns 'Insecure' Chinese Mobile Gear," *VentureBeat*, February 16, 2018, https://venturebeat.com/2018/02/16/zte-chases-5g-growth-in-japan-as-u-s-shuns-insecure-chinese-mobile-gear/.

[394] Brown and Singh, "China's Technology Transfer Strategy."

[395] This language is taken from a proposal to the ITU by a state block composed of China, Russia, Saudi Arabia, Algeria, Sudan, Egypt, and the United Arab Emirates (UAE). The proposal, withdrawn after its release, states "Internet governance shall be effected through the development and application by governments," and that member states shall have "the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance." For more details, see Violet Blue, "WCIT-12 Leak Shows Russia, China, Others Seek to Define 'Government-Controlled Internet'," ZDNet, December 12, 2012. https://www.zdnet.com/article/wcit-12-leak-shows-russia-china-others-seek-to-define-government-controlled-internet/.

sign the update, effectively defeating the effort.[396] The developing countries' support for China's position strongly suggests that the growing international presence of PRC investment and telecommunications firms influences these nations' stances on international standards.[397] At the very least, it provides cover and legitimacy for nations explicitly seeking to build a more restrictive internet.

Europe

China has emerged as a major contributor to European standards governing IoT development. This involvement is due in large part to Sino-European market integration, particularly within the telecommunications industry. For example, Huawei maintains a presence in every EU member state, and has spearheaded numerous key infrastructure development projects within Europe.[398] Huawei also maintains a robust lobbying presence within EU member states, as well as the EU organization as whole.[399] Moreover, many European governments are eager to do business in China's vast IoT marketplace, which incentivizes them to lobby for IoT standards that are compatible with China's equipment.[400]

China has participated in EU roundtable discussions on the future of EU telecom regulations since 2015,[401] in part to develop a unified global framework that can be used for all IoT devices.[402] At a signing session for a joint China-EU 5G Association memorandum, Lu Xi, the Deputy Director of MIIT's Technology Department, stressed that technology and standards exchange between China and the EU will "lay the foundation for the development of a unified global 5G standard."[403]

[396] Ackerman, "The U.N. Fought the Internet–And the Internet Won."
[397] For the complete list of countries who signed and refused to sign the Final Acts of WCIT2012, see "Signatories of the Final Acts: 89," WCIT2012, http://www.itu.int/osg/wcit-12/highlights/signatories.html.
[398] François Godement and Abigaël Vasselier, "China at the Gates: A New Power Audit of EU-China Relations," European Council on Foreign Relations, December 1, 2017, http://www.ecfr.eu/publications/summary/china_eu_power_audit7242#_ftn157.
[399] Godement and Vasselier, "China at the Gates."
[400] Godement and Vasselier, "China at the Gates."
[401] Claudia Vernotti, "China's Growing Interest for EU Digital Regulation: More Efforts in Promoting Full and Transparent Cooperation with China on 5G are Needed," *China-EU Newsletter*, April 27, 2016, http://www.chinaeu.eu/chinas-growing-interest-for-eu-digital-regulation-more-efforts-in-promoting-full-and-transparent-cooperation-with-china-on-5g-are-needed/.
[402] "中国 5G 推进组与欧盟 5G 基础设施协会签署 5G 合作备忘录" [China's 5G Promotion Delegation Signs 5G Cooperation Memorandum with EU 5G Infrastructure Association], Xinhua 新华, September 30, 2015, http://www.cac.gov.cn/2015-09/30/m_1116725267.htm.
[403] [China's 5G Promotion Delegation Signs 5G Cooperation Memorandum with EU 5G Infrastructure Association], Xinhua 新华.

A 2015 Sino-European summit on the future of 5G telecommunications technology identified five initiatives that China and Europe could undertake to develop 5G infrastructure:[404]

1) Building international consensus on the "concepts, basic functions, key technologies, and development progress of 5G technology"
2) Jointly researching 5G technologies
3) Promoting global standardization for 5G technologies, as well as other organizations such as the ITU.
4) Identifying the best radio frequency bands to meet spectrum requirements for 5G technologies.
5) Discussing "related services and applications" for 5G technologies, particularly in the field of IoT.

China appears to view cooperation with the EU in standards development as an important means of influencing global 5G standards. A 2014 joint white paper jointly released by China and the EU stressed the importance of cooperation in standards development in bringing the IoT market to maturity.[405] This sentiment was echoed in a 2017 white paper released by CAICT, which observed that creating a "unified digital marketplace" was critical to building a sustainable IoT infrastructure.[406] CAICT has also underscored the need to deepen and expand Sino-European cooperation on standards development, with the goal of influencing standards at the global level, particularly via the ITU and the 3GPP.[407]

It is likely that continued Sino-European cooperation on developing 5G standards will strongly impact the types of hardware used in 5G and IoT infrastructure globally. Combined, China and Europe make up a sizable portion of the global IoT marketplace. By 2020, the mobile device market in China is expected to reach 1.76 trillion RMB ($279.5 billion),[408] and the European IoT market is slated to grow to $131.2 billion by 2019.[409] If China and the EU were to homogenize their IoT standards, it is likely that many devices sold globally will comply with standards approved and pushed by the Chinese government. Many European telecommunications firms, like

[404] "中欧共推 5G 全球标准化" [China and Europe Push 5G Global Standardization], Liaocheng Science and Technology Bureau 聊城市科学技术局, September 30, 2015, http://www.lcskjj.gov.cn/News_View.asp?NewsID=1570.

[405] "China-EU Joint White Paper on Internet of Things Identification," EU-China IoT Advisory Group, October 31, 2014 19, http://www.miit.gov.cn/newweb/n1146312/n1146909/n1146991/n1648536/c3489529/part/3489530.pdf.

[406] "5G 经济社会影响白皮" [5G Economic and Social Impact White Paper], China Academy of Information and Communications Technology (CAICT) 中国信息通信研究院, October 31, 2014, http://www.caict.ac.cn/kxyj/qwfb/bps/201706/P020170711295172767080.pdf.

[407] "5G Cooperation and Progress in China," China Academy of Information and Communications Technology (CAICT) 中国信息通信研究院, April 8, 2016, http://www.chinaeu.eu/wp-content/uploads/2016/04/mazhigang-5G-Progress-and-Cooperation-in-China-20160408.pdf.

[408] "预测：2020 年中国移动物联网市场规模将达 1.76 万亿" [Forecast: The Scale of China's Mobile Internet of Things Market Will Reach 1.76 Trillion Yuan by 2020], Jiemian News 界面新闻, December 20, 2017, https://www.jiemian.com/article/1830845.html.

[409] "Europe Internet-of-Things (IoT) and Machine-to-Machine (M2M) Communication Market," Micromarket Monitor, accessed May 19, 2018, http://www.micromarketmonitor.com/market/europe-internet-of-things-iot-and-machine-to-machine-m2m-communication-2767638760.html.

Ericsson, have an extensive operating presence within the United States[410] meaning that Sino-European cooperation in standards development will likely directly impact the types of 5G and IoT hardware used in the United States as well.

Leveraging Market Size

China's domestically-developed standards wield considerable influence even absent international adoption. In 2003, China issued the Wired Authentication and Privacy Infrastructure (WAPI), a PRC National Standard for Wireless LANs (GB 15629.11-2003), prohibiting the import, manufacture, and sale of Wi-Fi gear that did not comply with this specification.[411] WAPI was developed as a competitor to Wi-Fi, reportedly because of Chinese concerns about the security of the Wi-Fi encryption protocol;[412] however, China refused to allow examination of the WAPI encryption algorithm, citing "national secrets." Hoping to make WAPI an international standard, China introduced it to the International Organization for Standardization. Though it came close to adoption at the ISO, it was ultimately rejected in favor of the IEEE 802.11i standard, a result that caused the Chinese delegation to walk out of global talks.[413] Many analysts believed that China's concern over the protocol stemmed primarily from a desire to control the communications technology and possibly to advantage domestic manufacturers, who would be paid royalties for the use of the standard. As the former director of the French standards body AFNOR put it, "The main specificity of the WAPI was to let Chinese authorities have access to the communications and eventually control them."[414] Chinese technology commentary from the period viewed WAPI as a contest between the United States and China that China failed.[415]

While unsuccessful in its push for international adoption, in 2009, China began requiring that new WLAN equipment support WAPI, and the MIIT began encouraging mobile phone makers to include the protocol.[416] This means that a wide range of devices are manufactured to include support for the WAPI protocol despite it not being fully understood or vetted for security.

The WAPI Industry Alliance, an industry group founded to promote the technology, has again been active at the ISO. In 2017, China won ISO certification for the WAPI Industry Alliance-led TRAIS-X technology.[417] Chinese news reports stress TRAIS-X as a "fundamental innovation

[410] "About Us," Ericsson, accessed May 19, 2018, https://www.ericsson.com/en/about-us/history/places/north-america/usa.

[411] Richard Shim, "China Implements New Wi-Fi Security Standard," https://www.cnet.com/news/china-implements-new-wi-fi-security-standard/.

[412] U.S. International Trade Commission, *China: Intellectual Property Infringement, Indigenous Innovation Policies, and Frameworks for Measuring the Effects on the U.S. Economy*, Investigation No. 332-514, USITC Publication 4199 (amended), November 2010.

[413] "China Walks out of Meeting to Resolve Bitter Feud over World Wireless Encryption Standard," *The Age*, June 10, 2006, https://www.theage.com.au/news/Technology/China-walks-out-of-meeting-to-resolve-bitter-feud-over-world-wireless-encryption-standard/2006/05/30/1148754947518.html.

[414] Olivier Peyrat, "China's Standardization Strategies."

[415] "WAPI 产生偏于国家主导化 中美对垒标准战略" ["WAPI Is Biased towards State Dominance: US-China Confrontation on Standards Strategy"] Tech.QQ.com, December 31, 2005, http://tech.qq.com/a/20051231/000148.htm.

[416] Owen Fletcher, "Years on, China Pushes WAPI in Mobile Phones," *IDG News Service*, May 8, 2009, https://www.cio.com/article/2428329/infrastructure/years-on--china-pushes-wapi-in-mobile-phones.html.

[417] The Industry Alliance is composed of members Xidian Jietong, the National Engineering Laboratory for Wireless Network Security Technologies, the National Commercial Password Detection Center, Tianjin Radio Monitoring

technology of the Internet of Things" and the fact that it has "completely independent intellectual property rights."[418] Recalling the "failure" of the WAPI standards, reporting heralded the adoption as an international standard technical specifications as "another major breakthrough for China in the key core technology areas of the global Internet of Things" with implications for spreading China's "advanced network security infrastructure technologies" to aid in "global network security."

Compelling and Exploiting Local-Foreign Corporate Cooperation

China is also known for coercing foreign corporations into cooperative agreements with Chinese companies in exchange for market access. ZTE has partnered with Qualcomm[419] and China Mobile on trials based on the 3GPP 5G New Radio (NR) specifications (in the sub-6 GHz mid-band spectrum).[420] Huawei has partnered with Intel on 5G interoperability development testing,[421] which adds to the two companies' existing partnership on high-performance computing.[422] Several major European telecommunications firms such as Nokia and Ericsson have participated in 5G development research projects which have ties to what was China's 863 Program (863 计划) for state high-tech development.[423]

Case Studies: Tactics in Action

Narrowband Internet of Things

China's extensive role in shaping of standards governing Narrowband Internet of Things (NB-IoT) provides an instructive example of the PRC's *modus operandi* for influencing international technology standards. NB-IoT is a narrowband radio networking technology that runs independently of the Long-Term Evolution (LTE) wireless communication networks.[424] By

Station, and the National Radio Monitoring Center Testing Center, https://www.yicaiglobal.com/news/chinese-iot-safety-technology-trais-x-receives-iso-certification.

[418] "我国物联网安全关键技术 TRAIS-X 成国际标准" ["Chinese Key Internet of Things Technology TRAIS-X Becomes International Standard"], Xinhua Net 新华网, October 23, 2017. http://www.xinhuanet.com/tech/2017-10/23/c_1121844149.htm.

[419] "Qualcomm, ZTE and China Mobile Announce Collaboration on 5G NR Trials at 3.5 GHz to Accelerate Wide-Scale 5G Deployments in China," ZTE Corporation, February 23, 2017, http://www.zte.com.cn/global/about/press-center/news/201702Ma/0223ma.

[420] Robert Triggs, "Qualcomm, ZTE, and China Mobile Test World's First 3GPP End-to-End 5G NR Connection," Android Authority, November 17, 2017, https://www.androidauthority.com/qualcomm-zte-china-mobile-5g-trial-814959//.

[421] "Huawei Joins Intel in 5G Collaboration on NR based Interoperability Development Testing," Huawei Corporation, September 22, 2017, http://www.huawei.com/en/press-events/news/2017/9/Huawei-5G-collaboration-Intel.

[422] "Huawei and Intel Sign a MOU to Accelerate HPC Innovation," Huawei Corporation, April 25, 2017, http://www.huawei.com/en/press-events/news/2017/4/Huawei-Intel-Sign-MOU.

[423] "5G Cooperation and Progress in China," China Academy of Information and Communications Technology (CAICT) 中国信息通信研究院, April 8, 2016, http://www.chinaeu.eu/wp-content/uploads/2016/04/mazhigang-5G-Progress-and-Cooperation-in-China-20160408.pdf.

[424] "3GPP Low Power Wide Area Technologies," GSM Association, October 2016, https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf; Brian Ray, "What is Narrowband IoT (NB-IoT)? Explanation and 5 Business Benefits," IoT For All, May 9, 2017, https://www.iotforall.com/what-is-narrowband-iot-nb-iot//.

transmitting independently or on previously unused KhZ bands, IoT devices connected to NB-IoT use significantly less power and bandwidth than conventional networked devices.[425]

China was among the first countries to develop a functioning NB-IoT network, which it implemented in the IoT testbed city of Wuxi beginning in 2016.[426] With Wuxi serving as an ongoing proof of concept, the government began devoting more resources to deploying NB-IoT at scale, including an initial 35 billion RMB ($5 billion) effort to cover Hongshan in an NB-IoT network.[427] This has been manifested in a number of state planning notices and documents, including the "MIIT Comprehensive Plan for Promoting the Construction and Development of the Internet of Things" (工业和信息化部办公厅关于全面推进移动物联网（NB-IoT）建设发展的通知).[428] The plan states MIIT's goal of making China a "leader international standards research," and outlines plans for the continued spread of NB-IoT services.[429] Currently, NB-IoT networks have been implemented in several major cities and demonstrative regions throughout China, which are mainly focused utilities such as smart gas, water metering, street lighting and parking.[430]

China's government-backed telecommunications providers strongly emphasized their role in developing NB-IoT by submitting suggestions for standards revisions through the 3GPP. Developers such as Huawei touted themselves as being vigorous promoters of the commercialization of NB-IoT, and regarded their ability to influence standards as being a critical indicator of its leadership status in the field.[431] By the time the core 3GPP Release 13 standard for NB-IoT was finalized in June 2016, Huawei had established itself as the most prolific contributor to the new standards regime.[432] Huawei submitted 1,008 proposals, which constituted 31.5% of the 3,205 proposals submitted by all companies. Of the 447 total approved proposals, Huawei's 184 proposals comprised 41%.[433] In June 2016, 3GPP completed the standardization of NB-IOT,

[425] Ray, "What is Narrowband IoT (NB-IoT)?"

[426] "China's First NB-IoT Network Made in Wuxi," *China Daily,* December 28, 2016, http://www.chinadaily.com.cn/m/jiangsu/wuxi/2016-12/28/content_27809073.htm.

[427] "China's First NB-IoT Network Made in Wuxi," *China Daily,* December 28, 2016, http://www.chinadaily.com.cn/m/jiangsu/wuxi/2016-12/28/content_27809073.htm.

[428] Ministry of Industry and Informatization Technology of the People's Republic of China, "工业和信息化部办公厅关于全面推进移动物联网（NB-IoT）建设发展的通知" [MIIT General Office Notice Regarding Comprehensive Advancement of Mobile IoT (NB-IoT) Construction Development], June 16, 2017, http://www.miit.gov.cn/n1146290/n4388791/c5692751/content.html.

[429] MIIT, "工业和信息化部办公厅关于全面推进移动物联网（NB-IoT）建设发展的通知" [MIIT General Office Notice Regarding Comprehensive Advancement of Mobile IoT (NB-IoT) Construction Development].

[430] Flora Tang, "Why China is Leading NB-IoT Development Globally," Counterpoint Research, November 9, 2017, https://www.counterpointresearch.com/why-china-is-leading-nb-iot-development-globally//.

[431] "窄带物联网" [Narrow Band IoT], Huawei Technology Company, Ltd., accessed May 21, 2018, http://e.huawei.com/cn/solutions/technical/iot/nb-iot.

[432] Ling Jiwei 凌纪伟, ed., "物联网产业进入商业应用元年" [Internet of Things Industry Enters First Year of Commercial Application], *Economic Daily* 经济日报, May 31, 2018, http://www.xinhuanet.com/tech/2017-05/31/c_1121059375.htm.

[433] Ling, [IoT Industry Enters First Year of Commercial Application].

implementing these features into Release 13 (LTE Advanced Pro).[434] China's leading role in developing NB-IoT has enabled it to strongly influence global standards for NB-IoT Devices.[435]

China's early investments in NB-IoT technologies have enabled it to decisively shape the evolution of that industry. A 2016 assessment by the Global System for Mobile Communications Association (GSMA) named Huawei, China Unicom, and China Telecom as key players in NB-IoT development and deployment.[436] Subsequently, Huawei has been instrumental in setting up NB-IoT testing and certification centers abroad in places like Australia and Chile, which has further enabled them to influence the direction of the global NB-IoT ecosystem.[437] China's robust domestic NB-IoT infrastructure development and the extensive contributions of Chinese firms to international standards suggest that China is able to exert considerable leverage over that marketplace. This sentiment seems to be reflected in Chinese self-assessments of its position within the global NB-IoT industry. In an interview with Xinhua, Li Guangqian (李广乾), the Director of Research at the Development Research Center of the State Council (国务院发展研究中心信息中心), posited that Huawei currently "dominates" the NB-IoT market, which has had a "major impact on China's future IoT industry… and the development of the entire information industry."[438]

5G Networks

With commercial rollouts beginning in 2018 and scheduled to ramp up in 2019, the world is on the cusp of 5G. The countries with the largest and most reliable 5G networks will have a head start in developing the technologies that 5G enables–first among them, the IoT. China has laid a solid groundwork for a comprehensive rollout, relying on a whole-of-country approach that has created an entire ecosystem for domestically manufactured 5G technologies and furthered their inclusion in international technical standards. With ten times the 5G sites per person as in the United States, China appears likely to lead early 5G deployment.[439]

The international standards community is pushing to establish 5G specifications by 2018 for implementation in 2020,[440] an effort China hopes to help lead after playing only a limited role in previous generations of mobile technologies. China was not involved in the development of 2G; it championed one of three globally-recognized 3G standards and one of two global 4G standards, but neither was widely adopted, and no Chinese firms were among the top 10 owners of essential

[434] "Standardization of NB-IoT Completed," 3GPP, June 22, 2016, http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete.

[435] Tang, "Why China is Leading NB-IoT Development Globally."

[436] "NB-IoT Forum Update," GSM Association, November 2016, https://www.gsma.com/iot/wp-content/uploads/2016/11/Presentation-02.-Global-MIoT-Summit-Tokyo-Nov-2016-Chairs-slides-v0.2.pdf.

[437] Connie Reichert, "Huawei to Launch NB-IoT Testing and Certification Center in Australia," ZDNet, December 18, 2017, https://www.zdnet.com/article/huawei-to-launch-nb-iot-testing-and-certification-centre-in-australia/; "Huawei and Telefónica Announce to Launch NB-IoT Open Lab to Boost the Internet of Things," Huawei Corporation, June 15, 2017, http://www.huawei.com/en/press-events/news/2017/6/Huawei-Telefonica-NB-IoT-Open-Lab.

[438] Ling, [IoT Industry Enters First Year of Commercial Application].

[439] Dan Littmann, Phil Wilson, Craig Wigginton et al., "5G: The Chance to Lead for a Decade" (London: Deloitte, 2018), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf?mod=article_inline.

[440] Paul Nikolich, Chih-Lin I, Jouni Korhonen et al., "Standards for 5G and Beyond: Their Use Cases and Applications," *IEEE 5G Tech Focus* 1 (2), June 2017, https://5g.ieee.org/tech-focus/june-2017/standards-for-5g-and-beyond.

4G intellectual property rights.[441] Between its commercial and state-backed efforts, China has emerged as a global leader in 5G development through its R&D efforts, patents and international technical standards, and market share acquisition,[442] with companies positioned along the entire 5G supply chain.

China's state plans, including the 13th Five-Year Plan, the Made in China 2025 plan, the annual government work report, and the "New Generation Artificial Intelligence Development Plan (新一代人工智能发展规划)," highlight 5G as a key priority for Chinese science and technology development, aiming for commercialization by 2020. Many of these aspirational plans have translated into large-scale government-funded infrastructure projects to drive 5G growth and development. In 2011, the 973 Program began supporting next-generation mobile communications systems, and by 2014 the 863 Program had folded in a megaproject on "Initial Research on Implementation of 5G Mobile Communications Systems" (实施 5G 移动 通信 系统 先期 研究). In 2016, the "New Generation Broadband Wireless Mobile Communications" National Science Megaproject initiated China's 5G technology R&D testing, the first phase of which was completed by 2017. The National Science Megaprojects have three major projects relevant to 5G technologies, and China is expected to complete phases 2 and 3 of technological R&D testing by 2018.[443] It is unclear what phases 2 and 3 entail.

China is currently attempting to influence the next round of international standards governing 5G networks using a strategy very similar to its approach to influencing NB-IoT standards. China is moving to deploy 5G in an initial operating capacity before other nations while bolstering those efforts with favorable government policy. At the same time, China is working to influence 5G international standards and to deploy 5G infrastructure at scale. This collection of measures is designed to enable China to take advantage of a self-reinforcing cycle in which the first country to deploy 5G wields strong influence over international standards. Favorable international standards strengthen that country's ability to deploy 5G at scale, which further enhances its dominance over international standards. China began undertaking many of these measures early: Beyond the many 5G-related patents Chinese companies hold, China has already built the world's largest 5G test field in Beijing.[444]

China's race to deploy 5G in an initial operating capacity is no secret, and signals its intent and progress in deploying a mature 5G network. Many estimates now put China in the lead, ahead of the United States and South Korea,[445] including an April 2018 report prepared for CTIA, a U.S.

[441] Bien Perez, "China's Chance to Lead Global Innovation May Lie with 5G Mobile Technology Development," *South China Morning Post,* October 1, 2017, http://www.scmp.com/tech/enterprises/article/2113581/chinas-chance-lead-global-innovation-may-lie-5g-mobile-technology.

[442] Auchard and Jiang, "China's Huawei Set to Lead Global Charge to 5G Networks."

[443] Li Wenjuan 黎文娟, Qiao Biao 乔标, and Shao Liguo 邵立国, "中国 5G 发展现状与未来趋势," [The Current Status and Future Trends of China's 5G Development," *Study Times 学习时报*, February 22, 2017, reprinted on the website of the Office of the Central Cyberspace Affairs Commission, http://www.cac.gov.cn/2017-02/22/c_1120508575.htm.

[444] Lifang, ed. "China Focus: China Counting Down to 5G Commercialization," Xinhua Net 新华网, December 7, 2017, http://www.xinhuanet.com/english/2017-12/07/c_136808018.htm.

[445] Gambardella, "China Is Set to Lead in Global 5G Race."

wireless industry trade association.[446] This advantage is due in large part to strong government support and a top-down coordinated research effort.

Huawei started working on efforts to develop 5G as early as 2009 and began pre-commercial tests of its 5G network starting in 2017.[447] The company released its own 3GPP-standard chipset in what some are calling a move that rivals Qualcomm and Intel, and puts it in the ranks of global 5G chipset leaders alongside Nokia, Xilinx Apple, Samsung, and Mediatek.[448] This chipset, which the company claims is the world's first commercial chipset to meet 5G standards, is an emblem of the heavy investment China has put into 5G and into developing its own components so as to avoid reliance on outside suppliers.[449] This lead in developing 5G technologies has helped make Huawei a top contender for other nations looking to award contracts for initial 5G wireless network contracts, including South Korea, a potential upset for the country's homegrown Samsung Electronics Co.[450]

Throughout this process, Huawei worked closely with regulatory agencies and research organizations within the Chinese government, as well as foreign partners such as LG.[451] These nascent deployment efforts are hugely influential for international standards, since international governance bodies tend to draw upon lessons learned from existing infrastructure.

Both Huawei and ZTE have also moved quickly on transitionary technologies that aim to bridge 4G and 5G. Huawei is at present conducting live trials of 5G wireless links with UK partners BT and EE using a proposed mmWave radio interface standard called New Radio (NR). Already approved by the 3GPP standards committee, the NR access standard is part of the first wave of 5G standardization, which aims to be backwards-compatible with 4G LTE systems. The release of specifications from the 3GPP committee was viewed as "an important 5G technical hurdle to be cleared."[452] For its part, ZTE has unveiled proprietary "Pre5G" solutions that allow carriers to "fast-track" 5G by applying it to existing 4G LTE infrastructure. According to ZTE, carriers

[446] Analysys Mason and Recon Analytics, "Race to 5G Report," CTIA, April 16, 2018, https://www.ctia.org/news/race-to-5g-report.

[447] "3GPP 5G 预商用系统获世界互联网领先科技成果" [Huawei's 3GPP 5G Pre-Commercial System Receives World's Internet Leading Scientific Achievement Award], Huawei 华为, accessed May 23, 2018, http://www.huawei.com/cn/about-huawei/executives/articles/Huawei-3GPP-5G-Pre-commercial-System; "LG Uplus and Huawei Complete 5G Pre-Commercial Tests in Gangnam," Telegeography, November 27, 2017, https://www.telegeography.com/products/commsupdate/articles/2017/11/27/lg-uplus-and-huawei-complete-5g-pre-commercial-tests-in-gangnam/.

[448] Dave Burstein, "5G The Same Speed As 4G: Huawei $Billion 5G Chip," Wireless One, February 26, 2018, http://wirelessone.news/mimo-2/985-5g-the-same-speed-as-4g-huawei-5g; "5G Chipsets: Global Industry Analysis & Forecast 2018-2026 - Strategic Partnerships With System Integrators in Emerging Economies," Cision PR Newswire, July 4, 2018, https://www.prnewswire.com/news-releases/5g-chipsets-global-industry-analysis--forecast-2018-2026---strategic-partnerships-with-system-integrators-in-emerging-economies-300675986.html.

[449] Arjun Kharpal, "Huawei Unveils Its First 5G Chip in a Challenge to Qualcomm and Intel," CNBC, February 25, 2018, https://www.cnbc.com/2018/02/25/huawei-unveils-5g-chipset-at-mobile-world-congress.html.

[450] Sam Kim, "Huawei May Beat Samsung to 5G in Its Own Backyard," *Bloomberg*, July 15, 2018, https://www.bloomberg.com/news/articles/2018-07-15/huawei-pushes-to-upset-samsung-in-south-korea-s-5g-network-race.

[451] [Huawei's 3GPP 5G Pre-Commercial System Receives World's Internet Leading Scientific Achievement Award], Huawei 华为; "LG Uplus and Huawei Complete 5G Pre-Commercial Tests in Gangnam," Telegeography.

[452] Richard Wilson, "Comment: US and China Lead Europe in the 5G Race," ElectronicsWeekly.com, March 16, 2018, https://www.electronicsweekly.com/news/comment-us-china-lead-europe-5g-race-2018-03/.

including SoftBank, China Mobile, and Telefonica have deployed this proprietary technology across more than 40 networks in 30 countries.[453]

ZTE's chief technology officer has singled out 5G and IoT as "core strategies" for ZTE, fields in which the company aims to become a global pioneer.[454] As an example of its progress in these areas, a January 9, 2017 press release reported ZTE's increased efforts in "key 5G technologies" and progress in channel coding, massive MIMO, network virtualization and slicing, and accurate positioning, technologies that are particularly important for a smart "Internet of Vehicles."[455] This investment has yielded significant returns: the two companies own the most intellectual property rights on 5G among Chinese entities, positioning them favorably for continued market advantage once 5G becomes the new mobile communications standard.[456]

China's telecommunications manufacturers are coordinating with its carriers to roll out 5G at maximum possible speed. In early 2016, ZTE joined with ten other China Mobile partners in a 5G Joint Innovation Lab, an effort the two noted would "deepen and broaden ZTE's partnership with China Mobile."[457] The lab's purpose is to combine resources across the telecommunications industry "in order to facilitate 4G-to-5G evolution and create a virtuous circle for innovation."[458] This lab involves close coordination with the IMT-2020 (5G) Promotion group, the state-backed group in China responsible for leading 5G technology development. The lab's partners promise to take part in the promotion group's 5G tests and "to promote 5G candidate technology validation, standards development, and industrial chain construction."[459] A ZTE executive vice president cited the lab as a vector through which "Chinese enterprises will be given more say and play a greater role in global 5G standardization and industrialization."[460] Later in 2016, ZTE announced a partnership with China Unicom, another of China's three state-backed carriers, on joint 5G and IoT innovation.[461]

The *People's Daily Online* quoted a Beijing-based IT expert on the impact of this R&D effort on China's influence in formulating international 5G standards, saying that while "in the past, China was merely following the technology framework designed by foreign competitors," things have changed because of China's R&D advantage. Today, "as an early starter in researching the technology, China is likely to have a bigger voice in formulating international 5G standards."[462] This has already proven true: while Western companies will likely still own the majority of 5G

[453] "ZTE Moves to No. 1 in World Intellectual Property Organization's Patent Table," Cision PR Newswire.

[454] "China Unicom and ZTE Sign Strategic Cooperation Agreement on Joint 5G and IoT Innovation," ZTE Corporation (press release), August 16, 2016, http://www.zte.com.cn/global/about/press-center/news/201608ma/20160816ma.

[455] "ZTE Joins 5GAA," ZTE Corporation (press release).

[456] Bien Perez, "China's Chance to Lead Global Innovation May Lie with 5G Mobile Technology Development," CNBC, October 2, 2017, https://www.cnbc.com/2017/10/02/chinas-chance-to-lead-global-innovation-may-lie-with-5g-mobile-technology-development.html.

[457] "ZTE Proud to Be Launch Partner in China Mobile's 5G Joint Innovation Lab (JIL)," ZTE Corporation (press release).

[458] Ibid.

[459] Ibid.

[460] Ibid.

[461] "China Unicom and ZTE Sign Strategic Cooperation Agreement on Joint 5G and IoT Innovation," ZTE Corporation (press release).

[462] "China Set to Take 5G Lead," originally published in *Global Times*, June 20, 2017, http://en.people.cn/n3/2017/0620/c90000-9230800.html on 17 April 2018.

standards-essential patents,[463] the balance is beginning to tip. China's significant progress in developing 5G technologies has won their inclusion in international standards, a trend that is the fruit of this whole-of-country effort and one that will likely be replicated with even higher success in future technological pushes.

Huawei has been behind a new error-control technique known as polar codes for the enhanced Mobile Broadband (eMBB) service category within 5G,[464] a technology for which it holds most of the core patents.[465] Polar codes face two more mature competing technologies: low-density parity-check (LDPC), which Qualcomm dominates, and Turbo, which has long been favored in Europe, though has fallen behind LDPC in recent years.

The U.S.-backed standard and the China-backed standard came head to head in a key 3GPP meeting in November 2016. In an effort to ensure that Huawei's standard would be accepted, the Chinese government pressured Chinese companies to back polar codes, resulting in a standoff that one standards expert present described as a "tense fight that lasted past midnight."[466] The fight ended in a compromise: ultimately, 59 companies voted in favor of China's polar codes, which were selected as the official coding method for control channel functions, while LDPC was selected for eMBB data channels. Absent major changes, this means that any certified 5G mobile cellular technology will have a polar code module or chipset inside.[467] While the compromise arguably gave Huawei the less significant channel, Chinese media heralded the victory as proving that China was taking part in standard-setting for 5G,[468] and it positions the company to earn royalties and wield greater leverage in future standards negotiations. Huawei itself celebrated the accomplishment and the inventor of the technology in a July 2018 ceremony, calling attention to its role as "a major contributor to 5G standards, and a core patent holder."[469]

While China's international influence efforts in 5G are still underway, emerging Chinese dominance in the international standards of 5G infrastructure are likely to bring about serious implications for the broader development of the IoT. Beijing's efforts to influence international 5G standards bear more than a passing resemblance to the ones it used to seize a considerable

[463] Josh Chin, Sarah Krouse, and Dan Strumpf, "The 5G Race: China and U.S. Battle to Control World's Fastest Wireless Internet," *Wall Street Journal*, September 9, 2018, https://www.wsj.com/articles/the-5g-race-china-and-u-s-battle-to-control-worlds-fastest-wireless-internet-1536516373.

[464] "Parity-Check Polar Coding for 5G and Beyond," Huazi Zhang, Rong Li, Jian Wang et al., Huawei Technologies Co., Ltd., January 11, 2018, https://arxiv.org/pdf/1801.03616.pdf.

[465] Wu Mingzhou, "Lenovo's Middle-Aged Crisis: Trapped in the "Voting Gate" Was Forced to Blame and Was Also [SIC]," WestDollar.com (sourced from "international financial newspaper"), May 16, 2018, http://westdollar.com/sbdm/finance/news/1344,20180515872375671.html?qrqm=cjdd.

[466] Chin, Krouse, and Strumpf, "The 5G Race."

[467] Alan Carlton, "Surprise! Polar Codes Are Coming in From the Cold," *ComputerWorld*, December 22, 2016, https://www.computerworld.com/article/3151866/mobile-wireless/surprise-polar-codes-are-coming-in-from-the-cold.html.

[468] "Shenzhen-based Huawei to Lead the Way in 5G," NewsGD.com, November 21, 2016, http://www.newsgd.com/news/2016-11/21/content_160107749.htm, "Huawei Successfully Bids for 5G Core Standard," YiCai Global, March 24, 2017, https://www.yicaiglobal.com/news/huawei-successfully-bids-5g-core-standard.

[469] "Huawei Recognizes Dr. Erdal Arikan, the Father of Polar Codes, for his Dedication to Basic Research and Exploration," Huawei (press release), July 26, 2018, https://www.huawei.com/en/press-events/news/2018/7/Huawei-Dr-Erdal-Arikan-Polar-Codes.

advantage in NB-IoT, suggesting that Chinese officials place a high premium on dominating the nascent field.

Key Points of Contention

The dramatic differences between the U.S. and Chinese approaches to standardization have led to several key differences in philosophical and technical preferences for international standardization of the IoT and 5G network deployment. A number of these differences are characterized briefly below.

Multi-Stakeholder Model of Internet Governance

A key philosophical difference between China's approach to standardization and internet governance and the United States is China's desire to move away from the multi-stakeholder model that has until now been a prominent feature of global technology standardization. China, along with many other developing countries "argued for the stronger anchoring of the Internet Governance Forum in the UN system, which would imply a more prominent role for governments."[470]

The ultimate effect of such a shift away from the existing multi-stakeholder model would be to disenfranchise non-state actors from the standardization process, even though the majority of internet infrastructure remains in private hands. This comports with China's assertion of "internet sovereignty (网络主权)," which stresses that nations have a right to own their own cyberspace.[471] It also grants significant additional voting influence to China, as its growing largesse through the Belt and Road Initiative has won it a number of emerging market nation-state allies, whose votes carry weight in the UN system but not in manufacturer-led bodies like 3GPP, where the weighted voting system has meant that even when Chinese companies like Huawei win a numerical majority of votes, they fail to defeat companies like Qualcomm.[472]

5G Frequency

The deployment of 5G networks at scale fundamentally relies on millimeter waves, and will ultimately require a dedicated band of frequencies to function. The international community remains divided on which frequencies to use for 5G: China and Europe favor low frequency bands (<6GHz), while the United States favors high-frequency bands (>24GHz, also known as millimeter wave or mmWave).[473] The high-frequency option offers much more availability in unused bandwidth but bears the burden of intrinsic technical challenges. Signals do not travel as far and can be blocked by obstacles including trees, buildings, and interference from rain, meaning that a

[470] Jovan Kurbalija, "An Introduction to Internet Governance," DiploFoundation, (Msida, DiploFoundation, 2014) https://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf.

[471] "尊重国家网络主权 [Respecting National Network Sovereignty], originally published via the People's Daily 人民日报, February 17, 2017, http://www.gov.cn/zhengce/2016-02/17/content_5042042.htm.

[472] Wu Mingzhou, "Lenovo's Middle-Aged Crisis: Trapping 'Vote Gates' Forced to Banishment and Being Removed from Constant Generation," *Westdollar*, May 16, 2018, http://westdollar.com/sbdm/finance/news/1344,20180515872375671.html?qrqm=cjdd.

[473] "5G Spectrum Recommendations," 4G Americas, August 2015, http://www.5gamericas.org/files/6514/3930/9262/4G_Americas_5G_Spectrum_Recommendations_White_Paper.pdf.

denser cell network will be necessary.[474] The low frequency option will require less investment in infrastructure and may make it easier to achieve nationwide coverage faster.

While the FCC has begun auctioning higher-frequency bands for use, China may be moving more quickly towards broader approval of low-frequency bands worldwide. Some analysts believe that China is seeking a first-mover advantage by "rolling out 5G at low frequencies fast to scale up the supply chain and lower equipment cost for the rest of the world…to pre-empt mmWave from gaining scale ahead and become the tech of choice by other markets."[475]

The dispute over 5G frequency is unlikely to be resolved until 2019, when the World Radiocommunications Conference 2019[476] is expected to set the agenda for which band of frequencies 5G will use.[477] In the meantime, however, operators and stakeholders have settled upon the best (or worst) kind of compromise by adopting a standard that attempts to please all parties but instead defers decision-making: Release 15, a global 5G standard that will make use of both sub-6 GHz and mmWave spectrum bands.[478]

Digital Object Architecture

Digital Object Architecture, a technical framework for IoT devices, remains a notable point of contention in the international arena. At its core, Digital Object Architecture (DOA) is a "general architecture for a distributed information storage, location and retrieval system running over the Internet," complete with unique, persistent identifiers and other information for devices that could help secure and track IoT devices.[479] DOA would be especially applicable to IoT devices, especially given the large number of IoT devices expected to proliferate in the coming years. Some participant nations in the ITU are "seeking to ensure that a proposal called Digital Object Architecture (DOA) is adopted as the global standard for IoT devices, and that the ITU is the entity authorized to administer the DOA's Global Handle Registry."[480]

Other nations, however, have gone further. Citing privacy and security reasons, some nations are seeking a recommendation from the ITU's Telecommunication Standardization Sector (ITU-T) proposing that DOA should become not just an IoT addressing and tracking system, but the sole global IoT addressing system. According to Wiley & Rein's blog, this would "violate long-held

[474] Allan Holmes, "5G Wireless Pits Cities against Telecoms and Their Friends in the FCC," The Center for Public Integrity, March 2, 2018, https://www.publicintegrity.org/2018/03/02/21475/5g-wireless-pits-cities-against-telecoms-and-their-friends-fcc.

[475] "Telecom Services: The Geopolitics of 5G and IoT," Jeffries Franchise Note, September 14, 2017, https://www.jefferies.com/CMSFiles/Jefferies.com/files/Insights/TelecomServ.pdf.

[476] "About the World Radiocommunications Conference," ITU, accessed May 23, 2018, https://www.itu.int/en/ITU-R/conferences/wrc/2019/Pages/default.aspx.

[477] Houlin Zhao, "How ITU Helps to Create a New Mobile Era via 5G," *ITU News*, February 28, 2018, http://news.itu.int/itu-helps-create-new-mobile-era-via-5g//.

[478] Andrei Frumusanu, "3GPP Completes First 5G NR Specification for Release 15," *Anandtech*, December 21, 2017, https://www.anandtech.com/show/12182/3gpp-completes-first-5g-nr-specification-for-release-15; "Qualcomm Announces 5G NR mmWave Prototype to Accelerate Mobile Deployments for Smartphones," Qualcomm, Inc., September 11, 2017, https://www.qualcomm.com/news/releases/2017/09/11/qualcomm-announces-5g-nr-mmwave-prototype-accelerate-mobile-deployments.

[479] "Overview of the Digital Object Architecture (DOA)," Internet Society, October 26, 2016, https://www.internetsociety.org/resources/doc/2016/overview-of-the-digital-object-architecture-doa/.

[480] Wiley Rein LLP, "ITU IoT Standards: Gateway to Government Control?" WileyConnect, September 20, 2016, https://www.wileyconnect.com/home/2016/9/20/itu-iot-standards-gateway-to-government-control.

principles of technology neutrality in ITU-T Recommendations."[481] Approval of DOA as a core IoT technology could restrict the free flow of information across borders and enable pervasive surveillance of IoT users. As written, the existing DOA proposal could set "…geographical boundaries on a previously borderless Internet. And if DO identifiers are used to supersede current identifiers in mobile handsets (IMEIs) as some have suggested, or if device registration is required, such tracking could extend to people as well."[482]

The massive surveillance potential of DOA has led some activists and ITU member states to argue that ITU is too closed a political organization to handle this type of standardization, and that DOA should be handed off to a multi-stakeholder organization.[483]

Chinese experts have expressed interest in DOA. In December 2017, China held its first DOA Development Forum (首届 DOA 技术应用论坛) in Beijing. The Forum was co-organized (联合主办) by MIIT's Electronic Technology Information Research Institute (ETIRI /国家工业信息安全发展研究中心; aka 工业和信息化部电子科学技术情报研究所), Content Digital Innovation Technology Co., Ltd. (北京中数创新科技股份有限公司 or CDI), and the Corporation for Handle Services in China (北京西恩多纳信息技术有限公司).[484] ETIRI is a primary intelligence research institute for China's defense industry.[485]

Implications for the United States

Standardization is generally regarded as a solution to a coordination problem: a positive development that allows different parties and competitors to obtain mutual benefit and reduce costs by abiding by an agreed-upon set of rules and practices. Standardization is a welcome process for the IoT sector, especially given the fragmented state of IoT development around the world.

Unfortunately, the actual process of standardization is far less simple and far more given to competition. While standardization of the IoT would be economically better, various parties gain differently from adoption of different standards, and each party can be expected to back their own standard right up to the point of adoption. Standardization is therefore a long, belabored process of consensus building and considered political maneuver.

[481] Ibid.

[482] Ibid.

[483] "Digital Object Architecture and IoT standardization," Exeter University Department of Politics, January 28, 2018, http://www.internetpolicystreams.com/news/item/362-digital-object-architecture-and-iot-standardisation.

[484] "全球首届 "DOA 技术应用论坛"在京成功召开" [World's First 'DOA Technology Application Forum' Successfully Held in Beijing], Xinhua 新华, December 12, 2017, http://www.xinhuanet.com/money/2017-12/12/c_129763755.htm; "全球首秀！徐工智能供应链亮相全球"DOA 技术应用论坛," [World Premiere! XCMG's Intelligent Supply Chain Unveiled the Global 'DOA Technology Application Forum'], XCMG 徐工集团, December 12, 2017, http://www.xcmg.com/gongying/news/521970.htm; "信软司参加数字对象架构技术应用论坛" [Software Firms Participate in Digital Object Architecture Application Forum], Ministry of Industry and Information Technology of the People's Republic of China 中华人民共和国工业和信息化部, December 12, 2017, http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057656/n3057660/c5949726/content.html.

[485] "招聘信息: 工业和信息化部电子科学技术情报研究所招聘公告" [Recruitment Information Ministry of Industry and Information Technology Electronic Science and Technology Information Institute Recruitment], University of Science and Technology Beijing 北京科技大学机电信息楼, May 12, 2016, http://scce.ustb.edu.cn/article.action?categoryId=47&boardaId=0&articleId=2240.

Much of what the United States is (or is not) doing in international standards developing organizations stands in opposition to Chinese actions. Wherever the United States has been decentralized in its approach to international standards, China is centralized. Where the United States has pulled back from participation, let industry groups take the initiative, or sent small delegations, China has sent large, coordinated groups of government and industry and pushed for a greater leadership role. Where the United States embraces multi-stakeholder models, China pushes for multilateralism. In total, these actions are shifting the balance away from a U.S.-led model of standardization into one in which China has a greater say.

China's scholars, technical experts, and government officials understand the nature and importance of this type of standardization competition. Chinese scholars at key state-funded institutions view standardization from a competitive standpoint: academics at a Ministry of Education State Key Laboratory at Northwestern Polytechnical University (西北工业大学) have undertaken studies of game theory and standardization work in manufacturing enterprises, reflecting the degree of government emphasis on influencing and winning the battle over standards.[486] Multiple segments of China's government and state-led enterprises are encouraged to see standardization work as a way to increase China's economic competitiveness and international influence.[487]

As a result, China's standardization efforts both at home and abroad are critical manifestations of state-led efforts to ensure China becomes the world's premier innovator in the IoT and the infrastructure needed to deploy the IoT on an expansive scale. Overall, Chinese officials have adopted an approach using market share and development progress to justify its preferred international standards, while using those same standards to lock in Chinese market and technical advantages for the benefit of Chinese companies.

In contrast, U.S. efforts at IoT and 5G standardization are more decentralized. No unified, comprehensive legal mandates exist to hold IoT manufacturers accountable for IoT security or data privacy, and major U.S. telecom providers continue to vie with each other in rolling out different types of 5G trial deployments. One subject matter expert regarded U.S. participation in major 5G international standards bodies as a simple matter of preserving the status quo, confident that major U.S. telecoms would continue to play a leading role in determining future standards almost by default.[488]

Chinese dominance of the IoT and its attendant infrastructure through standardization will have far-reaching consequences for both U.S. economic interests and national security. Some analysts project that by some measures the IoT will generate some $470 billion in revenues by 2020,[489] and 5G is estimated to add up to $12.3 trillion in revenues around the world.[490] Chinese-dictated international standards would give Chinese manufacturers a head start on seizing market share in

[486] Jiang Jianjun, Wang Junbiao, Li Shuguang, and Zhang Jianxin, "Game Theory Strategy for Information Standardization Work in Manufacturing Enterprise," in Yan Xiu-Tian, Jiang Chengyu, and Benoit Eynard, eds., *Advanced Design and Manufacture to Gain a Competitive Edge* (London: Springer, 2008).

[487] "Special Project Action Plan for Internet of Things Development," 8-9.

[488] In-person interview with cybersecurity and telecommunications subject matter expert, April 2018.

[489] Herbert Blum, Darren Jackson, Velu Sinha, and Paul Smith, "Close to the Core: Telcos' Competitive Advantage in the Internet of Things," Bain and Company, February 24, 2017, http://www.bain.com/publications/articles/telcos-competitive-advantage-in-the-internet-of-things.aspx.

[490] Qualcomm, "The 5G Economy: How 5G will Impact Global Industries, The Economy, and You," *MIT Technology Review*, March 1, 2017, https://www.technologyreview.com/s/603770/the-5g-economy-how-5g-will-impact-global-industries-the-economy-and-you/.

these sectors, adding to their already substantial market advantages and leading to lost IP and licensing revenue for U.S. firms.

From a national security perspective, adoption of Chinese-backed international standards offers Beijing unparalleled opportunities to compromise trillions of potential future IoT devices through security vulnerabilities it has researched and locked in though international standards bodies, with little or no built-in transparency on these vulnerabilities.[491] While the entire world might still see absolute economic gains from IoT standardization even under China's preferred constructs, it is readily apparent that China would gain far more comparatively under a Chinese-backed standards regime.

Recommendations

Several policy recommendations arise from the implications described above. Although the following steps are not an exhaustive documentation of possible countermeasures, together they represent an initial approach to countering the negative impacts of China's concerted push to influence international standards.

1. Conduct additional open source reporting and research on China's international standards efforts.

While the United States need not adopt a centralized approach to counter China's push for adoption of its preferred international standards, a deeper appreciation for the nuances of China's *modus operandi* is a prerequisite for any effective action to compete with or counter it. Further documentation of China's efforts to capture international standards and broad dissemination of this information to parties with a role in generating international standards would inform more vigorous debate and encourage more transparency in the standards that China pushes.

2. Encourage more U.S. participation in international standards committees through additional funding and incentives.

While some subject matter experts regard U.S. participation in international standards bodies as a thankless task with little reward, the work could perhaps take on greater prestige if given more emphasis through government incentives. Standardization work is almost certainly mundane and laborious, but restructured incentives could help motivate more U.S. technical experts to engage in the dirty but indispensable work of international standards bureaucracy. More funding for organizations like NIST that specialize in standardization could help incentivize more U.S. experts to undertake standardization work in international settings.

[491] For more information on the lack of transparency in Chinese security standards, see Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," Center for Strategic and International Studies, August 2018, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF.

3. Where acceptable, adopt proposals and processes agreed upon by multi-stakeholder international standardization bodies like the IETF while continuing to counter Chinese attempts to re-define internet governance as a matter of national sovereignty that requires the devolution of control to nation-states.

U.S. government bodies should adopt proposals and guidelines from non-profit, multi-stakeholder international standardization bodies like the Internet Engineering Task Force (IETF). This strengthens the multi-stakeholder model of international standardization that includes a larger set of public and private organizations, rather than state-centric organizations like the UN ITU. Lending legitimacy to the multi-stakeholder model has two main benefits: first, it provides more ample opportunities for innovation by soliciting and incorporating more feedback from private and public stakeholders, and second, it bypasses state-centric influence efforts deployed by China's whole-of-nation approach to international standardization. China is focused on influencing standards at ITU, which is a body organized around nation-states and increasingly susceptible to Chinese package deals to develop foreign national internet and telecom infrastructure. Within the ITU and other international standards development organizations, the United States should continue to strongly resist Chinese attempts to compel agreement with proposals that re-define internet governance as a matter of national sovereignty and empower state governments to become the sole regulators of the internet, a move that many authoritarian governments embrace.

4. Create a government-industry advisory body charged with studying corporate foreign interactions in the interest of national security.

U.S. companies with operations in China are frequently strongly incentivized to cooperate with Chinese partners as an implicit condition for further market penetration in China's massive IoT sector. This is a pernicious prospect for many reasons, one of which is that U.S. companies may feel more compelled to abide by Chinese standards or back them in international forums. While there may be little that can (or necessarily should) be done structurally to discourage U.S. companies from participating in the Chinese market, the U.S. government should more fully exercise its mandate to provide for the common defense by advising these companies of technology areas like dual-use technology in which their actions may have broader negative national security implications, especially in international standardization.

Chapter 3: Unauthorized Access and Chinese Research into IoT Security Vulnerabilities

As the Chinese government continues to prioritize IoT development at the state level through government-backed funding and international standards-setting efforts, it is also simultaneously supporting wide-ranging research efforts into IoT security vulnerabilities. Technical research on IoT security vulnerabilities in China has become a high priority for both public and private organizations, which draw support from government research programs and funding.

While IoT vulnerability research is often undertaken with the primary goal of enhancing Chinese information security, it should be considered "dual-use" in that such knowledge can directly feed into unauthorized efforts to access, surveil, or penetrate IoT devices. Sophisticated technical knowledge of hardware or software vulnerabilities in an IoT device, or supporting elements like cloud storage systems, can just as easily be used to attack these systems as to protect them. Ostensibly civilian-led and defensive IoT research can increase the odds of success for China's offensive computer network operations.

Despite increasing attention surrounding IoT security vulnerabilities, inherent problems in IoT devices and software significantly amplify the risks of unauthorized access to IoT devices. Low barriers to entry and limited regulatory standards for IoT devices mean that companies are strongly encouraged to enter the growing IoT market but have little incentive to make their devices secure. The large number of different manufacturers makes it harder for suppliers to push security updates and patches for products. Finally, the widespread use of IoT devices and the ease of IoT device discovery on the open internet means the potential negative impact for countless users if and when devices are compromised is incredibly high: a malicious actor can compile a list of affected and vulnerable devices around the world in minutes using publicly available tools such as SHODAN whenever an IoT device vulnerability is publicly disclosed. Chinese-manufactured IoT devices are frequent targets for unauthorized access, thanks in large part to these inherent vulnerabilities.

Given the potential these systemic security weaknesses hold to enable exploitation and unauthorized use of IoT devices, as well as China's long history of intertwining its military and civilian network and information security research ecosystems, even China's defensive government-supported IoT security research deserves strict scrutiny. The high degree of collaboration already observed between civilian academic and government research organizations, private sector firms, and military and defense industrial organizations in Chinese IoT security research suggests a strong governmental interest in harnessing the ability to gain unauthorized access to IoT devices and networks.

Existing Security Vulnerabilities in the IoT: A Primer

Security in the IoT is designed to protect privacy, defined as the assurance of confidentiality and control over information disclosure,[492] which is in turn based upon the principle of authorization. The National Institute of Standards and Technology (NIST) defines authorization as "access privileges granted to a user, program, or process or the act of granting those privileges"[493]—in other words, who is allowed to access what information and in what manner.[494] Authorization is especially prominent in the widely-applied "confidentiality, integrity, and availability" (CIA) model of information security, which regards authorization as a critical component of confidentiality. [495] For instance, NIST defines "confidentiality" as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[496]

Any exploitation of security vulnerabilities in the IoT by an unauthorized party to access a device in an unauthorized manner is an example of unauthorized access and a breach of security that could lead to an intrusion on privacy. While there are potentially infinite ways to gain unauthorized access to IoT devices including physical means, this chapter focuses primarily on non-physical means, namely technical compromise of information systems.

At a fundamental level, the IoT is especially vulnerable to technical compromise because nearly every component of the IoT is a potential target for attack. Components of a conventional network that do not gather or transmit information across a network connection directly to other network components, like monitors, keyboards, and other computer peripherals, are not potential attack surfaces. Linking previously unconnected physical items to a network and to the internet, however, potentially exposes all of these connected devices to unauthorized access attempts, greatly expanding the threat surface for any given IoT network.[497] IoT devices deployed at the edge of a network in large numbers present more potential attack surfaces for unauthorized access.[498]

Many IoT devices are also vulnerable thanks to their small size and high mobility. Some IoT devices are too small or mobile to accommodate more comprehensive built-in security measures.[499] For instance, automated network-connected hand-sanitation systems may be able to automatically send out a product resupply order when sanitizer liquid runs low, but may not have

[492] Many information security specialists regard "privacy" as the assurance of confidentiality, while "security" is a set of measures meant to protect privacy. For a more thorough treatment of the distinction, see Houbing Song, Glenn A. Fink, and Sabina Jeschke, eds., *Security and Privacy in Cyber-Physical Systems* (Hoboken, NJ: Wiley-IEEE Press, 2017), 1-3.

[493] United States Department of Commerce, National Institute of Standards and Technology, "Glossary," *NIST Computer Security Resource Center,* accessed July 7, 2018, https://csrc.nist.gov/Glossary/?term=3081#AlphaIndexDiv.

[494] Dorothy E. Denning, *Information Warfare and Security* (Boston, MA: Addison-Wesley, 2001), 41.

[495] Multiple academic works and information security textbooks refer to the CIA model of information security, and even though the CIA model has been improved upon in subsequent years, current models continue to include the three basic components of the CIA model. See Dorothy E. Denning, *Information Warfare and Security*, 41.

[496] United States Department of Commerce, National Institute of Standards and Technology, "Glossary."

[497] David Hanes, Gonzalo Salgueiro, and Rob Barton, *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things* (Indianapolis, IN: Cisco Press, 2017), Chapter 1.

[498] William Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (Addison-Wesley Professional, 2015), Chapter 16, Section 5.

[499] Sabella, Irons-Mclean, and Yannuzzi, *Orchestrating and Automating Security,* Chapter 1.

the circuit board space to accommodate more complex security and authentication protocols.[500] Illustrative examples of vulnerabilities in small devices have already been identified. In 2017, the FDA announced that small implantable cardiac devices have vulnerabilities that could allow an attacker to steal information or alter device performance, and recommended that patients keep the devices connected in order to receive the necessary security updates.[501] These small IoT devices often represent the weakest potential link in a network's security architecture, to say nothing of the threat they may pose to the end user on their own.

Other IoT devices are vulnerable because cost considerations discourage effective security measures. Low-cost devices typically have few security features because chip manufacturers have strong incentives to produce firmware and software as quickly and cheaply as possible, and device manufacturers frequently choose system chips based on price and functionality.[502] This often means that potentially countless low-cost devices deployed at the edges of IoT networks are especially vulnerable to attack. Less-secure IoT devices have already been exploited: in 2017, attackers were able to steal more than ten gigabytes of data from a U.S. casino by exfiltrating it through an IoT-enabled fish tank.[503] Reports indicated that the fish tank lacked top-flight security features, allowing a person inside the company to upload sensitive data to the fish tank's internal memory and exfiltrate the information using the tank's internet connection.[504]

The comparatively low production cost of IoT devices has enticed a vast number of IoT device and platform manufacturers to enter the market, which makes it difficult to distribute and deploy security updates across many different IoT devices and platforms. Many IoT deployments use sensors, gateways, applications, cloud infrastructure, and other components sourced from a variety of different vendors and companies,[505] each with their own proprietary security management systems that can make it difficult to deploy patches or updates efficiently. In 2016, malware known as the Mirai botnet began to take advantage of multiple different types of devices connected to various networks, scanning the internet for IoT devices that used default security credentials. It commandeered some one hundred thousand of these devices, and used them to carry out a distributed denial of service (DDoS) attack against DynDNS that shut down many popular websites.[506] Another similar botnet named IoTroop targeting different brands of wireless Internet Protocol (IP) cameras was identified in late 2017.[507]

Beyond the devices themselves, many IoT networks are fundamentally vulnerable because so many devices can connect to each other through dynamic, decentralized, and distributed network

[500] Ibid., Chapter 3.

[501] United States Food and Drug Administration, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication," January 9, 2017, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.

[502] William Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud* (Addison-Wesley Professional, 2015), Chapter 16, Section 5.

[503] Alex Schiffer, "How a Fish Tank Helped Hack a Casino," *Washington Post,* July 21, 2017, https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?noredirect=on.

[504] Yolanda Bobeldijk, "They Got in through the Fish Tank: The Threat of Shadow IT," *Financial News,* July 18, 2017, https://www.fnlondon.com/articles/they-got-in-through-the-fish-tank-firms-wrestle-with-shadow-it-20170718.

[505] Sabella, Irons-Mclean, and Yannuzzi, *Orchestrating and Automating Security,* Chapter 5.

[506] Ibid., Chapter 3.

[507] "A New IoT Botnet Storm is Coming," Check Point Research, October 19, 2017, https://research.checkpoint.com/new-iot-botnet-storm-coming/.

connections. The vast number of heterogeneous devices communicating with each other or joining and leaving networks makes it difficult for any security authority to exclude malicious actors or compromised devices from gaining access to a network.[508] Highly fluid IoT networks with vast numbers of connected devices that frequently cannot defend themselves adequately are difficult to monitor and can be easily compromised.

Many of these inherent weaknesses in the IoT are ripe opportunities for unauthorized access, and examples of unauthorized access to IoT devices are likely to increase substantially given the dramatically increased use of connected hardware in various sectors. As companies link more and more devices to the internet and to each other through networks, attackers will inevitably see more and more opportunities to gain unauthorized access to IoT devices in nearly every sector that uses IoT devices. For instance, malicious actors were able to take control of a Jeep vehicle remotely through weak default security measures in the vehicle's internet-connected multimedia system in 2015.[509] Penetration testing specialists demonstrated a flaw in a Samsung smart refrigerator that could result in theft of Gmail login credentials.[510]

The various security challenges inherent in the IoT and the increasing exploitation of these holes could generate profoundly negative and widely disparate consequences for end users and operators of IoT devices and networks. Unauthorized virtual access to industrial control systems has already led to destructive effects in the physical world: the Stuxnet malware destroyed Iranian nuclear processing equipment in 2010,[511] and a Russian cyberattack shut down substantial portions of the Ukrainian power grid in 2016.[512] Aside from industrial control systems, unauthorized access to health care devices could kill patients and exploitation of smart car vulnerabilities could kill drivers and pedestrians alike, among other examples of possible misuse of data and devices that could have dire consequences. The future destructive potential of unauthorized access to IoT devices appears potentially limitless.

Known Vulnerabilities in Chinese IoT Devices

Chinese IoT devices have frequently been accessed by third parties, sometimes maliciously and without permission, due to compromises and outright errors on the part of the companies designing them. In late 2016, for example, the Chinese IoT device manufacturer Hangzhou Xiongmai Technology Co. Ltd. (杭州雄迈信息技术有限公司 or Xiongmai) was forced to initiate a large-scale recall of its webcams after a number of them were commandeered by the Mirai botnet and used to launch DDoS attacks against major DNS providers.[513] Information security researchers examining the Mirai botnet discovered that Xiongmai devices were routinely released without

[508] Mung Chiang, Bharath Balasubramanian, and Flavio Bonomi, *Fog for 5G and IoT* (Hoboken, NJ: John Wiley and Sons, 2017), 261-281.
[509] Alex Drozhzhin, "Black Hat USA 2015: The Full Story of How That Jeep Was Hacked," *Kaspersky Lab Daily,* August 6, 2015, https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/.
[510] Colin Neagle, "Smart Refrigerator Hack Exposes Gmail Login Credentials," *NetworkWorld,* August 26, 2015, https://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.
[511] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum,* February 26, 2013, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
[512] Andy Greenberg, "'Crash Override': The Malware That Took down a Power Grid," *Wired*, June 12, 2017, https://www.wired.com/story/crash-override-malware/.
[513] Sijia Jiang and Jim Finkle, "China's Xiongmai to Recall up to 10,000 Webcams after Hack," Reuters, October 25, 2016, https://www.reuters.com/article/us-cyber-attacks-china-idUSKCN12P1TT.

even basic security features, making them particularly ripe targets for malicious actors looking to commandeer internet-connected devices.[514] Devices by Zhejiang Dahua Technology Co. Ltd. (浙江大华技术股份有限公司 or Dahua) and Hangzhou Hikvision Digital Technology Co. Ltd. (杭州海康威视数字技术股份有限公司 or Hikvision) were also compromised.[515] Although Hikvision released a patch for its devices,[516] both Dahua and Hikvision continued to attract notice from the information security community for the unusually poor security of their IoT devices, with one analyst from Chinese firm NSFocus singling them out in May 2017 for having the highest number of exposed network surveillance devices.[517]

Even when vulnerable Chinese devices are not used for network attack purposes via botnets, vulnerabilities in Chinese devices may offer avenues for unauthorized access. In 2017, for example, it was discovered that more than 175,000 IoT cameras around the world produced by Shenzhen Neo Electronics Co. Ltd. (深圳市丽欧电子有限公司) were remotely accessible and viewable due to basic vulnerabilities in the devices' access protocols.[518] That same year, IoT device maker Shenzhen DblTek Technology Co. Ltd. (深圳市得伯乐科技有限公司 or DblTek) was discovered to have intentionally left a backdoor enabling remote access in its VoIP products, ostensibly for debugging purposes, which the company has not remediated.[519]

Remediation measures put in place to provide over-the-air updates to the firmware of Chinese IoT devices may present security and privacy challenges of their own. In 2016, information security researchers discovered that firmware update software made by Shanghai ADUPS Technology Co. Ltd. (上海广升信息技术股份有限公司 or ADUPS) was in fact secretly siphoning private data from those devices and returning it to the company's servers in China.[520] ADUPS's firmware update software is currently in use on more than 700 million low-end mobile phones and IoT devices around the globe, including devices in the United States. As of 2017, however, despite this malicious behavior being widely publicized in international media, the company continues to deploy firmware update software that can be used to engage in unauthorized data collection. Similarly, in 2016, reports surfaced revealing that Shenzhen Foscam Intelligent Technology Co. Ltd (深圳市福斯康姆智能科技有限公司 or Foscam), a major Chinese maker of IoT cameras with a U.S. subsidiary, was selling IoT cameras that surreptitiously phoned home to Foscam's

[514] Roi Perez, "Chinese IoT Device Manufacturer Recalls Products Amidst Mass DDoS Attacks," *SC Media UK*, October 25, 2016, https://www.scmagazineuk.com/chinese-iot-device-manufacturer-recalls-products-amidst-mass-ddos-attacks/article/568303/.

[515] Drew FitzGerald, "Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks," *Wall Street Journal*, September 30, 2016, https://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428.

[516] Chris Brook, "Hikvision Patches Backdoor in IP Cameras," *Threatpost*, May 8, 2017, https://threatpost.com/hikvision-patches-backdoor-in-ip-cameras/125522/.

[517] "Dahua, Hikvision IoT Devices under Siege," Krebs on Security, March 10, 2017, https://krebsonsecurity.com/2017/03/dahua-hikvision-iot-devices-under-siege/; "Exposed IoT Assets in China Analysis," NSFocus, May 26, 2017, https://blog.nsfocusglobal.com/categories/exposed-iot-assets-in-china-analysis/.

[518] Danny Palmer, "75,000 IoT Cameras Can Be Remotely Hacked Thanks to Flaw, Says Security Researcher," *ZDNet*, July 31, 2017, https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/.

[519] John Leyden, "We Found a Hidden Backdoor in Chinese Internet of Things Devices–Researchers," *The Register*, March 2, 2017, https://www.theregister.co.uk/2017/03/02/chinese_iot_kit_backdoor_claims/.

[520] Patrick Howell O'Neill, "Chinese Tech Firm Continues to Secretly Siphon Data from Android Phones," *Cyberscoop*, July 25, 2017, https://www.cyberscoop.com/android-malware-blu-kryptowire-adups-software/.

servers around the world.[521] Although the camera's administration settings ostensibly offered a way to disable this behavior, the company admitted that even with the feature set to "disabled," the camera would still constantly beacon out to Foscam's servers.[522]

While a comprehensive study on the relative vulnerabilities of Chinese IoT devices remains outside the scope of this report, the examples above illustrate that Chinese IoT devices are at least as susceptible to unauthorized access as those from other suppliers, and may in fact be more susceptible. Regardless, the impact of security vulnerabilities and the threat of unauthorized access to Chinese IoT devices may be greater given the wide usage of the compromised Chinese IoT devices identified above.

Chinese Research into IoT Security Vulnerabilities

China's IoT experts and policymakers have been mindful of the IoT's security vulnerabilities from an early stage. MIIT's China Academy of Telecommunication Research identified security as one of the core IoT development challenges needing further government study and consideration in its 2011 "IoT White Paper," and called for a full assessment of the security threats, data leakage vulnerabilities, and privacy threats facing IoT systems.[523] It also recommended the creation of systems for IoT layered protection, security evaluation, and risk assessment.[524] Soon after, China released its 12th Five Year Plan Development Plan for the Internet of Things, which identified "strengthening information security" as one of the main IoT development tasks for the next five years. The specific tasks outlined in the development plan included:

- Strengthening R&D in IoT security technology, focusing on areas like privacy protection, access control, key management, secure routing, and intrusion detection;
- Creating and improving an IoT security system made up of government organizations, industry supervisory departments, and third-party testing agencies; and
- Strengthening network infrastructure defense.

China continued to identify IoT security as a core development task in both the 2013 Special Project Action Plan for Internet of Things Development and the 2016 Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum. Both documents emphasize the need to improve the country's ability to ensure IoT security by focusing on R&D and commercialization of IoT security technologies and the creation of a sound IoT security system that focuses in particular on IoT network testing and security assessments.[525]

While much of China's emphasis on improving IoT security is expressed in defensive terms, information security research is inherently agnostic and can be used to secure IoT devices or gain unauthorized access to them. For instance, penetration testing, a legal and authorized attempt to locate and exploit vulnerabilities in information systems, is a mainstay of defensive information

[521] "This is Why People Fear the 'Internet of Things'," Krebs on Security, February 18, 2016, https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/.

[522] "This is Why People Fear the 'Internet of Things'," Krebs on Security.

[523] "物联网白皮书 (2011 年)" [2011 White Paper on IoT], China Academy of Telecommunication Research of MIIT 工业和信息化部电信研究院, May 2011, www.miit.gov.cn/newweb/n1146312/n1146909/n1146991/n1648536/c3489477/part/3489478.pdf.

[524] "2011 White Paper on IoT," China Academy of Telecommunication Research of MIIT.

[525] "Information and Communications Industry Development Plan (2016–2020) Internet of Things Addendum"; "Special Project Action Plan for Internet of Things Development."

warfare intended to strengthen the security of information systems.[526] Penetration testers, however, frequently use the same tools and approaches as malicious actors in an attempt to act and think like an attacker intent on gaining unauthorized access to a system.[527] Penetration testers and malicious attackers are only separated by fundamental but fragile differences, namely authorization, motivation, and intent.[528] In other words, information security research, including IoT security research, can just as easily be used to secure China's IoT or to gain unauthorized access to IoT devices around the world.

Beijing's strong rhetorical emphasis on IoT security is unsurprising given its attention to network security as a function of national security,[529] but China's extensive research into IoT vulnerabilities could also enable intelligence collection and cyberwarfare capabilities based upon unauthorized access. In fact, evidence strongly suggests that China's coercive apparatus supervises and directs the collection and release of vulnerabilities. China's government routinely publishes disclosures of software vulnerabilities via the Chinese National Vulnerability Database (国家信息安全漏洞库 or CNNVD) so that firms within the private sector can quickly identify and patch weak points within their security architectures.[530] However, analysis by the threat intelligence firm Recorded Future uncovered substantial evidence indicating that high-impact vulnerabilities were "routinely evaluated for their operational utility by the MSS before publication."[531] Anecdotal evidence also indicates that MIIT discourages Chinese security vendors from participating in international hacking competitions in order to stockpile vulnerabilities that would otherwise be disclosed to the international community.[532] It is likely that this practice of stockpiling vulnerabilities for exploitation extends to IoT products sold in U.S. markets.

Still, determining China's specific intent to use certain IoT vulnerabilities is extremely difficult, as the operational utility of IoT exploits is directly proportional to their secrecy prior to use.[533] Instead, examining the contours of Chinese IoT security research gives clues about what types of IoT vulnerabilities might later be exploited.

[526] For a description of the role of penetration testing in defensive information warfare, see Dorothy E. Denning, *Information Warfare and Security*, 38. For a definition of penetration testing, see Patrick Engebretson, *The Basics of Hacking and Penetration Testing,* 2nd ed. (Waltham, MA: Syngress, 2013), 1.
[527] Engebretson, *The Basics of Hacking and Penetration Testing*, 2-3.
[528] Ibid., 3-4.
[529] Yang Ting 杨婷, ed., "习近平: 把我国从网络大国建设成为网络强国" (Xi Jinping: Transform China from an Internet Great Power to a Strong Internet Power), Xinhua, February 27, 2014, http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm.
[530] The purpose of the CNNVD mirrors that of the United States' National Vulnerability Database (NVD): both are vulnerability repositories that private firms can utilize to secure their networks. However, the CNNVD's approach to collecting vulnerabilities differs from that of the NVD, as the CNNVD actively searches for vulnerabilities across the web as opposed to waiting for firms to disclose them, as is standard practice for the NVD. See Priscilla Moriuchi and Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," Recorded Future, November 17, 2018, https://go.recordedfuture.com/hubfs/reports/cta-2017-1114.pdf.
[531] Moriuchi and Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications"; Priscilla Moriuchi and Bill Ladd, "China Altered Public Vulnerability Data to Conceal MSS Influence," Recorded Future, March 9, 2018, https://go.recordedfuture.com/hubfs/reports/cta-2018-0309.pdf.
[532] Yingzhi Zhang, "China Discourages Its Hackers from Foreign Competitions so They Don't Help Others," *South China Morning Post*, March 21, 2018, https://www.scmp.com/tech/article/2138114/china-discourages-its-cybersecurity-experts-global-hacking-competitions.
[533] Interview with information security expert, July 2018.

Overview of Chinese IoT Security Research

IoT security research in China has exploded over the past half-decade as Chinese information security researchers have become acutely aware of the potential consequences of IoT security vulnerabilities. The China National Knowledge Infrastructure (CNKI) database indicates some 1,229 articles on IoT security were published in 2017, up from only 9 such articles in 2009.[534] While the overall body of Chinese IoT security research is extremely diverse, a number of important trends stand out that could enable unauthorized access.

Chinese IoT security experts are well-versed in the basic vulnerabilities of the IoT. In early 2013, engineers from Westone Information Industry (卫士通信息产业股份有限公司), a leader in China's information security industry and a subsidiary of the China Electronics Technology Group Corporation (CETC) defense electronics conglomerate, noted that the challenges of securing IoT systems were substantially greater due to their complexity. IoT networks have to secure a high number of access points at multiple layers within the system (e.g., the sensor level, data transmission, and application levels), and protect data integrity across a relatively long transmission path.[535]

More specifically, Chinese IoT security researchers have focused on attacks that take advantage of heterogeneous, dynamic, and decentralized IoT networks with multiple connected devices. Mobile ad-hoc networks (MANETs) comprised of wireless mobile nodes that communicate with each other without using pre-established network architecture are especially vulnerable to certain classes of packet-dropping network attacks like wormhole, sinkhole, or black- and gray-hole attacks that delete or discard important data in transit, thereby overloading a network and potentially causing a denial of service.[536] Multiple Chinese researchers have published articles on these types of attacks, including the protection of source nodes against wormhole attacks[537] and detection methods for gray-hole attacks.[538]

Likely the most important trend in Chinese IoT security research has been the development of algorithmic and machine learning techniques for the discovery of IoT vulnerabilities across a wide range of devices, such that one does not have to completely "reinvent the wheel" every time a new device is analyzed.[539] The development of "polymorphic" IoT worms—malicious code that can

[534] Data obtained through the China National Knowledge Infrastructure database by searching for "物联网" (Internet of Things) in combination with "安全" (security).

[535] Wang Huibo 王会波, Li Xin 李新, and Wu Bo 吴波, "物联网信息安全技术体系研究" (IoT Infosec Technical System), *信息安全与通信保密 Information Security and Communications Privacy* 233, no. 5, (2013): 98-101.

[536] See M. Krishna Prasanna and M. Neelakantappa, "Minimization of Gray-Hole Attack Effect for Secured Mobile Ad Hoc Networks," *International Journal of Pure and Applied Mathematics* 118, no. 24, (2018), 1-2; Harsh Kishore Mishra, "Wormhole Attack," presentation, Cyber Security II Semester, August 3, 2014, https://www.slideshare.net/HarshMishra3/wormhole-attack.

[537] Sun Lele 孙乐乐 and Yuan Jiabin 袁家斌, "物联网中抵抗虫洞攻击的源节点保护研究" (Protection of Source Node Position Against Wormhole Attacks in the Internet of Things), *计算机与数字工程 Computer and Digital Engineering* 41, no. 1, (2013): 85-88.

[538] Zhang Guanghua 张先华, Yang Yaohong 杨耀红, and Zhang Dongwen 张冬雯, "IPv6 物联网中灰洞攻击的检测方法" (Detection Method for Gray Hole Attack in IPv6 Internet of Things), *小型微型计算机系统 Journal of Chinese Computer Systems* 39, no. 7, (2018): 1504–1511.

[539] See, for example, Chang Qing 常青, Liu Zhongjin 刘中金, Wang Mengtao 王猛涛 et al., "VDNS: 一种跨平台的固件漏洞关联算法" (VDNS: An Algorithm for Cross-Platform Vulnerability Searching in Binary Firmware), *计算机研究与发展 Journal of Computer Research and Development* 53, no. 10 (2016): 2288-2298.

continue spreading across numerous devices within a network operating different forms of hardware and software, such as between a networked printer and a smart thermostat—is a critical field in IoT security research. A wide variety of research has been funded into not only algorithmic techniques for the discovery of IoT vulnerabilities across a wide variety of devices, but also the creation of highly variable network attack testing platforms necessary to accurately model how such worms would spread inside the varied topography of adversary networks.[540]

While such research can certainly be used for innocuous purposes, such as improved independent analysis of IoT devices, it is particularly useful in an offensive context. Advances in algorithmic vulnerability detection may enable the rapid investigation of an ever-growing range of devices as potential attack vectors for a given target entity, a process that has historically been painstaking due to the wide variety of firmware and hardware present within them. These vulnerabilities can then be used in the development of "polymorphic" worms containing malicious code designed to jump between dissimilar devices as they propagate within a network.

China's Burgeoning IoT Research Ecosystem

In addition to ongoing work on IoT vulnerabilities by China's longstanding information and network security research organizations, a number of dedicated laboratories and institutions have been founded in the past several years that devote themselves to IoT research, as described below. Relevant research is now conducted by a wide range of public and private entities, with varying focuses ranging from network and device resiliency to attack vector discovery, along with many other IoT-related topics that frequently have bearing on IoT security. Much of this research is conducted through efforts including one-off grants and research projects carried out by longstanding information security research laboratories and dedicated IoT laboratories and research institutions. Several key IoT-specific research entities are profiled below, including several carrying out security-related research.

Beijing Key Laboratory of IoT Information Security Technology (物联网信息安全技术北京市重点实验室)

Founded in 2015, the Beijing Key Laboratory of IoT Information Security Technology, hereafter the Beijing Key Laboratory, is housed within the Chinese Academy of Sciences' Institute of Information Engineering (中国科学院信息工程研究所 or CAS IIE). The key laboratory's work focuses on developing IoT security architecture for massive, heterogeneous networks.[541] This line of effort includes research into IoT-based vulnerabilities in industrial control system and critical infrastructure networks.[542] One particularly interesting line of vulnerability research carried out by the Beijing Key Laboratory centers on using algorithmic approaches to discover firmware

[540] Chang, Liu, Wang et al., "VDNS: An Algorithm for Cross-Platform Vulnerability Searching in Binary Firmware."

[541] "物联网信息安全技术北京市重点实验室" [Beijing Key Laboratory of Internet of Things Information Security], 北京科学技术委员会 Beijing Municipal Science and Technology Committee, accessed May 15, 2018, http://www.bjkjcxjd.org/news/detail/4677.

[542] "物联网信息安全技术北京市重点实验室 2016 年度开放课题申请指南" [Beijing Key Laboratory of Internet of Things Information Security Open Course Application Guidance for 2016], 中国科学院信息工程研究所 Chinese Academy of Sciences Institute of Information Engineering, accessed May 15, 2018 http://www.iie.ac.cn/xwdt_101144/tzgg/201512/t20151214_4493530.html.

vulnerabilities in a wide range of IoT equipment.[543] This research targets the fact that many IoT vendors use similar code to comprise their firmware according to CPU architectures in use, including in network equipment such as routers. The Beijing Key Laboratory also claims to provide security assessment services to industry partners, although a list of specific partners has not been disclosed.[544]

The Beijing Key Laboratory and its researchers frequently work with other CAS organizations, particularly the State Key Laboratory of Information Security (中国科学院信息工程研究所信息安全国家重点实验室 or SKLOIS), on a range of IoT security and vulnerability research. Indeed, many if not most Beijing Key Laboratory researchers are temporarily seconded from other laboratories and hold dual affiliations, usually with CAS organizations such as the University of the Chinese Academy of Sciences. The laboratory claims to fund joint research projects with not only domestic but also foreign IoT research entities, though it has not provided a list of its foreign partners.[545]

The Beijing Key Laboratory's research is also supported by a long list of non-military research grants, including the CAS State Priority Research Program (中国科学院战略性先导科技专项课题), China's National Key Technology Research and Development Program (国家重点研发计划), the 863 Program (国家高技术研究发展计划), the Beijing Science & Technology Commission Science and Technology Innovation Base (北京市科委科技创新基地培育与发展工程专项项目), the Beijing Municipal Education Commission (北京市教委科技计划), Beijing Technology and Business University (北京工商大学国有资产管理协同创新中心项目), the CAS Institute of Information Engineering (中国科学院信息工程研究所前瞻部署项目), the China Post-Doctoral Science Fund (中国博士后科学基金资助项目), the Hebei provincial government (河北省高等学校科学技术研究项目 and 河北省科技计划支撑项目), and the National Natural Science Foundation of China (国家自然科学基金项目).

Northwest University-Irdeto IoT Information Security Joint Laboratory (西北大学-爱迪德物联网信息安全联合实验室)

Irdeto is a major global digital development and information security firm headquartered in the Netherlands, and Northwest University (NWU) is one of China's leading comprehensive and scientific research universities.[546] The Irdeto-NWU joint laboratory is a partnership between NWU and Irdeto's Chinese subsidiary, Irdeto Technology (Beijing) Co., Ltd. (爱迪德技术北京有限公司). The NWU-Irdeto laboratory's research focuses primarily on IoT-relevant code protection and obfuscation measures, as well as techniques that might enable an adversary to analyze and potentially overcome those measures in an offensive context.

Irdeto's joint laboratory with NWU is one of three first established in 2009; Irdeto also established collaborative research agreements with the Beijing University of Posts and Telecommunications

[543] Chang, Liu, Wang et al., "VDNS: An Algorithm for Cross-Platform Vulnerability Searching in Binary Firmware."

[544] "Beijing Key Laboratory of Internet of Things Information Security," Beijing Municipal Science and Technology Committee.

[545] "Beijing Key Laboratory of Internet of Things Information Security Open Course Application Guidance for 2016."

[546] "Contact Us," Irdeto, accessed May 15, 2018, https://irdeto.com/contact-us.html.

(北京邮电大学) and the CAS State Key Laboratory of Information Security (中国科学院信息安全国家重点实验室 or SKLOIS).[547] Based on a survey of the NWU-Irdeto laboratory's published research over the years, it appears that the laboratory was first designed as more general information security research institution but then shifted to an exclusive IoT focus over time.[548] The laboratory's research receives a wide range of Chinese government funding, most notably from the National Natural Science Foundation and the Shaanxi government's provincial science and technology development funds.

Little is known about the laboratory's leadership, other than that Tang Zhanyong (汤战勇), a Northwest University professor, currently serves as the laboratory's deputy director.[549] Tang is a former employee of NSFocus, a "white-hat" Chinese information security firm that has historically been closely linked to the Chinese hacker group Xfocus and the former "Green Army" patriotic hacker group. Gu Yuanxiang (顾元祥), chief architect at Irdeto, is also linked to the laboratory and holds a visiting professorship at NWU.[550] Gu was one of the initial driving forces behind Irdeto's partnerships with Chinese research institutions after Irdeto established its China headquarters in 2007.[551]

Changzhou Liuguojun Vocational Technology College Information (Internet of Things) Engineering Department (常州刘国钧高职校信息(物联网)工程系)

Changzhou Liuguojun Vocational Technology College is a Changzhou-based technical school offering a list of technical specialties that has recently expanded to include IoT research and training. In August 2013, the college converted its Information Engineering Department into an IoT-focused entity.[552] This shift may have been in response to the Chinese government's increasing emphasis on the IoT during this same time period (as discussed above), and may thus represent an attempt to better meet governmental mandates and attract government funding. Although the institution has published some research relevant to IoT since that time, the IoT department has not established itself as a major research institution.

Yunnan Nationalities University Provincial Key Laboratory of IoT Applied Technology (云南民族大学云南省高校物联网应用技术重点实验室)

Yunnan Nationalities University is a major civilian research and teaching university located in the city of Kunming. In recent years, the university has become host to a Provincial Key Laboratory of IoT Applied Technology. Relatively little is known about the Provincial Key Laboratory's specific research agenda or history, although it appears to have been founded in 2014.[553] However,

[547] "40 Years of Irdeto," Irdeto, accessed May 15, 2018, https://irdeto.com/documents/Irdeto_40_year_book.pdf.

[548] Data obtained through searches of the China National Knowledge Infrastructure (CNKI).

[549] "汤战勇" [Tang Zhanyong], Northwest University School of Information and Technology, accessed May 15, 2018, http://ist.nwu.edu.cn/home/index/article/mid/5354/id/206965.html.

[550] Gu Yuanxiang, "The Intelligent Vehicle as a Hostile Environment," Irdeto, accessed May 15, 2018 https://issisp2017.github.io/assets/slides/intelligent_vehicle_hostile_env-issisp2017.pdf.

[551] "40 Years of Irdeto," Irdeto.

[552] "Changzhou Liuguojun Vocational Technology College," Baidu Baike, accessed May 15, 2018, https://baike.baidu.com/item/%E5%B8%B8%E5%B7%9E%E5%88%98%E5%9B%BD%E9%92%A7%E9%AB%98%E7%AD%89%E8%81%8C%E4%B8%9A%E6%8A%80%E6%9C%AF%E5%AD%A6%E6%A0%A1/6530474.

[553] "我校 '云南省高校普洱学院力学开放重点实验室'获批立项建设" [Our School's 'Yunnan Province Pu'er University Wins a Project Award to Develop a Key Laboratory], Pu'er University, July 4, 2014, http://www.peuni.cn/info/1052/2341.htm.

based on a review of academic writings and research activities published by affiliated individuals, the laboratory appears to place a considerable emphasis on military research.[554]

Researchers affiliated with the Provincial Key Laboratory have co-authored information security research with both offensive and defensive applications in partnership with scientists from multiple state-owned corporations that serve as part of the Chinese defense industrial base, including CETC and Aviation Industry Corporation of China (AVIC).[555] At one point, the laboratory oversaw a large-scale research project on "complex network applications and modeling research" (复杂网络模型与应用研究) and it has sponsored research on elliptic curve cryptography, both fields of study that have not only civilian but also military and security applications.[556]

Jiangnan University School of IoT Engineering (江南大学物联网工程学院)

Jiangnan University is a major civilian research university located in the city of Wuxi. The university's School of IoT Engineering was formed in 2010 through the merger of its former Schools of Communication and Control Engineering (通信与控制工程学院) and Information Engineering (信息工程学院). Much like its parent university, the School of IoT Engineering receives government funding for its research agenda from numerous sources, including 863 Program funding earmarked for technology sectors of importance to national security.

The School of IoT Engineering appears to have a robust international exchange program, including hosting visiting professors from Western countries. The school even indicates that it has a partnership with the major German multinational engineering and electronics company Bosch GmbH. The school's collaboration with Bosch appears to be centered on vehicular IoT services.[557]

Nanjing University of Posts and Telecommunications College of Internet of Things (南京邮电大学物联网学院)

Nanjing University of Posts and Telecommunications (NUPT) is one of China's foremost civilian science and technology universities with a long history of conducting government and military-sponsored defense technical research. NUPT's College of IoT is a teaching and research school founded in 2009 as a merger of NUPT's IoT Engineering (物联网工程系) and Network Engineering (网络工程系) programs.[558]

NUPT's IoT researchers are engaged in research for public commercial entities. NUPT's College of IoT is associated with the NUPT IoT Technology Park (南邮物联网科技园), a joint project of

[554] Data obtained through searches of the China National Knowledge Infrastructure (CNKI).

[555] Peng Wu 彭武, Huang Qi 黄琦, Meng Xiaojun 孟小娟, and Chen Junhua 陈君华, "基于多元信息融合的网络威胁动态评估" (A Dynamic Network Threat Assessment Method Based on Multi-Source Information Fusion), *中国电子科学研究院学报 Journal of CAEIT* 11, no. 3, (2016): 250–256.

[556] "蒋作" [Jiang Zuo], Yunnan Minzu University, April 4, 2018, http://202.203.158.67/web/58756/showartical?ArticalId=680518e6-e6a7-409f-a86c-5ac9e37800d8.

[557] "Home Page," Jiangnan University School of IoT Engineering, accessed May 15, 2018, http://iot.jiangnan.edu.cn/.

[558] "学院介绍," Nanjing University of Posts and Telecommunications, accessed May 15, 2018, ciot.njupt.edu.cn/1/list.html.

NUPT and the Nanjing Gulou District municipal government established in 2010.[559] Jiangsu NUPT IoT Technology Park Co., Ltd. (江苏南邮物联网科技园有限公司) is the primary corporate entity governing the park. The park appears to exist primarily to offer a commercialization avenue for the technical advances made by researchers affiliated with the college, but several dozen companies have already enrolled and the mandates of the national Special Project Action Plan for Internet of Things Development suggest that the park may be a locus of civil-military integration activities.

Xiamen University of Technology Provincial Key Laboratory of IoT Applied Technology (厦门理工学院福建省高校物联网应用技术重点实验室)

Xiamen University of Technology is a provincial public university in Fujian province. Since at least 2012, the university has housed a Provincial Key Laboratory of IoT Applied Technology. The Provincial Key Laboratory functions as a partnership between Xiamen University of Technology and the Xiamen Industrial Technology Research Institute (厦门产业技术研究院).[560]

Little is known about the Provincial Key Laboratory's research direction. Chen Xuhui (陈旭辉) currently serves as the Provincial Key Laboratory's director.[561] Chen also serves as the deputy director of Xiamen University of Technology's Department of Computer Science, and was once a postdoctoral fellow at Arizona State University. His research does not have a clear focus within the IoT space, though he has published work on the use of IoT for medical devices as well as work on protocol analysis with potential relevance to IoT security.[562]

The Civil-Military Overlap

When looking into Chinese organizations focused on IoT security research, one striking trend is the high degree of collaboration between civilian academic and government research organizations, private sector firms, and military and defense industrial organizations. These collaborative research efforts are funded through a wide variety of municipal, provincial, and national funding mechanisms, including the National 863 High-Tech R&D Program, which focused on crucial science and technology development goals with direct relevance to China's long-term national security, particularly in the realm of information technology. This coordination is centrally directed: the Special Project Action Plan for Internet of Things Development states that industry, military, and civilian government IoT research must all coordinate with one another, in keeping with the State Council's 2009 "Decision on Accelerating the Cultivation and Development of Strategic Emerging Industries" (关于加快培育和发展战略性新兴产业的决定) and the State Council's 2013 "Guiding Opinion on Promoting the Orderly and Healthy Development of the Internet of Things" (关于推进物联网有序健康发展的指导意见). In addition, the Special Project Action Plan stipulates that "superior IoT industry projects" should be brought into the defense

[559] "南邮物联网科技园" [NUPT IoT Technology Park], Baidu Baike, accessed May 15, 2018 https://baike.baidu.com/item/南邮物联网科技园/14690192.

[560] "第五届 "广联达杯" 全国高等院校工程算量软件大赛圆满落幕" [Fifth "Broad Alliance Cup" National High-Level School Engineering Software Competition Begins], Xiamen University of Technology, November 21, 2012, https://www.xmut.edu.cn/mtlg/201211/t20121122_175439.html.

[561] "Xiamen University of Technology," China Higher Education Student Information Network, accessed May 15, 2018, https://yz.chsi.com.cn/sch/schoolInfo--schId-302972497,categoryId-302972529.dhtml.

[562] "Xiamen University of Technology," China Higher Education Student Information Network.

ecosystem to derive military benefits from them.[563] According to the Plan, the NDRC, MIIT, and entities within the Central Military Commission are jointly in charge of ensuring the success of civil-military integration with China's growing IoT industry.

Many institutions specifically founded to carry out IoT research have explicit partnerships with defense institutions or receive government funding from projects known to focus on national security objectives.[564] Despite this high degree of concordance with China's plans for "civil-military integration" (军民结合 or CMI) in the IoT sector, in keeping with the Special Project Action Plan for Internet of Things Development, these organizations may use their status as civilian research organizations to engage in a wide array of international partnerships and collaboration in a manner that Chinese military institutions might not ordinarily be able to, potentially with U.S. entities.[565] Chinese research institutions are thus able to bring the benefits of foreign research and innovation directly into China's military research, development, and acquisitions (RD&A) ecosystem.

The civil-military overlap is evident in relationships between several of the IoT research organizations identified above. For instance, the Beijing Key Laboratory of IoT Information Security Technology appears to have direct ties to Chinese military research. The laboratory was apparently founded in response to the Special Project Action Plan for Internet of Things Development, which identified a need for more specialized government IoT research institutions, and which also directed that those institutions work to deepen CMI in the IoT space. Research from the Beijing Key Laboratory has on at least one occasion has been sponsored by the National Defense [Basic] Scientific Research Plan (国防科工局国防基础科研计划).[566]

Other institutions also have ties to military research. Researchers affiliated with the Jiangnan University School of IoT Engineering have conducted joint research with scientists from Chinese defense industrial organizations such as the China Shipbuilding Industry Corporation's 7th Research Institute (中国船舶重工集团公司第七研究院 or CSIC).[567] CSIC is a major state-owned naval defense conglomerate, and CSIC's 7th Research Institute is primarily focused on naval weapons development. The 7th Research Institute specifically boasts a number of ongoing CMI research initiatives in which Jiangnan University's IoT researchers may be participating.[568] Chinese government organizations performing national security work also appear to be actively

[563] "Special Project Action Plan for Internet of Things Development."

[564] See, for example, Lu Shichao 吕世超, Sun Limin 孙利民, Shi Zhiqiang 石志强, and Sun Degang 孙德刚, "关键基础设施中工业控制系统安全监管与防护探讨" (Discussion on Safety Supervision and Protection of Industrial Control Systems in Critical Infrastructure), *保密科学技术 Secrecy Science and Technology* 72, no. 9, (2016): 12-17.

[565] This phenomenon is commonly observed in more well-known Chinese defense companies, which frequently use multiple aliases to mask their ties to the PLA in order to obtain materials and cooperation from unwitting U.S. entities. Some of these companies (and their aliases) have been placed on an export ban list from the U.S. Department of Commerce. See "Addition of Certain Entities; and Modification of Entry on the Entity List," United States Department of Commerce, August 1, 2018, https://www.gpo.gov/fdsys/pkg/FR-2018-08-01/pdf/2018-16474.pdf.

[566] Lu, Sun, Shi, and Sun, "Discussion on Safety Supervision and Protection of Industrial Control Systems in Critical Infrastructure."

[567] Wang Haiying 王海颖, Liu Yi'an 刘以安, Xue Song 薛松, and Miao Lei 缪磊, "基于集对分析联系度的多传感器数据融合方法" (Multi-sensor Data Fusion Based on Connection Degree of Set Pair Analysis), *智能系统学报 CAAI Transactions on Intelligent Systems* 12, no. 1, (2017): 1-8.

[568] "中船重工第七研究院 (中国舰船研究院) 2017 招聘" [CSIC 7th Research Institute (China Warship Research Institute) 2017 Employment] YingJieSheng, March 6, 2017, http://www.yingjiesheng.com/job-002-502-857.html.

recruiting School of IoT Engineering students in order to bring their research talents into China's defense science and technology ecosystem.[569]

The Jiangnan University School of IoT Engineering is also known to house a specialized Laboratory of Information Confrontation and System Simulation (信息对抗与系统仿真实验室).[570] "Information confrontation" (信息对抗) is a specialized People's Liberation Army term of art that broadly encompasses offensive and defensive computer network operations (CNO) against a nation-state adversary in contexts ranging from full-on warfare to network reconnaissance and espionage operations during peacetime and crisis. Unlike the IoT engineering school itself, which is relatively public-facing, only a single public record of this laboratory's existence is publicly available.[571] No details about the laboratory's work have been disclosed aside from their work on the science of multi-sensor data fusion, an important area of military research due to its relevance to constructing effective next-generation C4ISR platforms.

The Nanjing University of Posts and Telecommunications has a long institutional history of providing research support for the Chinese military, and its College of IoT also appears to focus in part on training students headed for military IoT work.[572] The college has several main research focuses including next-generation communication network and Internet Protocol technologies, IoT network applications technologies, and sensor network technologies, all of which have both civilian and military applications.[573] Funding for the college's research comes from a variety of sources, including the Jiangsu provincial government and the 863 and 973 Programs. Much like the 863 Program, the 973 Program is designed to fund research that will one day give China a national advantage in critical technology sectors. NUPT's IoT college is responsible for a number of 973 Program projects, including "IoT Hybrid Information Fusion and Decision-making" (物联网混杂信息融合与决策研究) and "Cognitive Coordination and Network Capacity Optimization" (认知协同与网络容量优化理论).[574]

The civil-military overlap described above conforms with China's view of IoT security research as having national security implications, instead of a simple commercial concern. As Chinese military researchers have argued, the IoT has increasing relevance to battlefield operations and must be understood in the context of promoting linkages between civilian technical development and military end users, frequently referred to as "civil-military integration" (军民结合 or CMI).[575]

[569] "通知公告," [Notices and Bulletins], Jiangnan University School of IoT Engineering, accessed May 15, 2018, http://iot.jiangnan.edu.cn/kxyj/tzgg/1.htm.
[570] Wang, Liu, Xue, and Miao "Multi-sensor Data Fusion Based on Connection Degree of Set Pair Analysis."
[571] Ibid.
[572] "物联网学院 2018 年研究生招生复试须知" [IoT School 2018 Graduate Student Recruitment Final Examination], Nanjing University of Posts and Telecommunications, accessed May 15, 2018, http://ciot.njupt.edu.cn/416/11/11/news.html.
[573] "南京邮电大学物联网学院" [Nanjing University of Posts and Telecommunications], Baidu Baike, accessed May 15, 2018, https://baike.baidu.com/item/%E5%8D%97%E4%BA%AC%E9%82%AE%E7%94%B5%E5%A4%A7%E5%AD%A6%E7%89%A9%E8%81%94%E7%BD%91%E5%AD%A6%E9%99%A2
[574] "南邮物联网科技园" [NUPT IoT Technology Park], Baidu Baike, accessed May 15, 2018 https://baike.baidu.com/item/南邮物联网科技园/14690192.
[575] Hao Jinjie 郝金杰, Ding Zhihong 丁志宏, Li Chunyu 李春雨, and Pang Yuning 庞钰宁, "物联网在军事远程机动任务中的应用研究" (Research on Application of Internet of Things in Army Remote Maneuver), *无线互联科技 Wireless Internet Technology* 24 (2017): 13.

Chinese military and defense industrial authors have also discussed the importance of IoT research for defense applications, such as the IoT's role in the implementation of the PLA's upcoming "integrated space-air-ground information network" (天地一体化信息网络).[576]

The Chinese government's decision to treat IoT security and technology development as a major national security priority is problematic in light of the high degree of integration between the Chinese and U.S. civilian IoT industries. U.S. consumers regularly make use of IoT devices designed or manufactured in China, entrusting them with access to potentially sensitive networks and data. However, as in other areas of network security, the Chinese government has explicitly enshrined in law the principle that the national security implications of emerging information technologies such as the IoT necessitate vesting the Chinese government, military, and intelligence agencies with the power to appropriate and inspect information systems and data at will (as discussed in greater detail in Chapter 4 and Appendix B). The Chinese government has given itself nearly unchecked legal powers to harness the data and supply chains of Chinese civilian firms for uses ranging from espionage to offensive operations. In some cases, Chinese leaders may even serve simultaneously as members of major IoT firms that are ostensibly private while at the same time holding government positions within China's national security bureaucracy.[577] This creates the potential for an unresolved critical tension between the commercial interests of Chinese firms wishing to sell IoT products in the United States and the security and privacy of U.S. citizens.

Operational Applications for IoT Vulnerability Research: Beyond Securing the IoT

China's IoT security research entities are part of a broader and increasingly fused civil-military research ecosystem that increases the chances that PRC intelligence and military actors will have access to any breakthroughs in IoT vulnerability research. Chinese intelligence and military organizations are already taking advantage of this extensive research ecosystem to make use of IoT security vulnerabilities. Several of these applications are described below.

Protecting Military Sensors from Unauthorized Access

Perhaps the most obvious use of Chinese IoT vulnerability research is to protect its own military sensors from unauthorized access. Numerous Chinese military and defense industrial authors have discussed the importance of IoT security research for the PLA's operations on the networked battlefields of the future, with some arguing that IoT technology is critical for the implementation of what will one day become the PLA's "integrated space-air-ground information network" (天地一体化信息网络). This "integrated space-air-ground information network" is a concept for next-generation PLA C4ISR operations that involves constant data streams between platforms at every level of the battlefield.[578] Towards this end, research conducted partly or wholly in the civilian

[576] Zeng Ye 曾业 and Zhou Yongjiang 周永将, "天地一体化信息网络天基物联网应用体系研究" (Space-based Internet of Things Applications Based on Integrated Ground-Air-Space Information Network), *现代导航 Modern Navigation* (2016): 372.

[577] See, for example, John Honovich, "Hikvision Exec Simultaneously Chinese Government Security Leader," *IPVM*, April 27, 2016, https://ipvm.com/reports/hikvision-cetc-mps.

[578] See, for example, Zeng and Zhou, "Space-based Internet of Things Applications Based on Integrated Ground-Air-Space Information Network," 372, and Hao, Ding, Li, and Pang, "Research on Application of Internet of Things in Army Remote Maneuver," 13-14.

sphere may later be "spun on" to the PLA's development through established civil-military integration channels.[579]

A wide range of PLA academic institutions conduct research on IoT technology, including the National University of Defense Technology (国防科技大学), PLA Army Engineering University (解放军陆军工程大学), PLA Logistics Engineering University (解放军后勤工程学院), PLA Equipment Academy (解放军装备学院), PLA Air Defense Academy (解放军防空兵学院), and PLA Military Economics Academy (解放军军事经济学院).[580] Chinese civilian and military IoT researchers have also published alongside researchers from a wide variety of state-owned defense conglomerates, including CETC and its 20th Research Institute, AVIC, the China Aerospace Science and Industry Corporation (CASIC), CSIC, and others. While this research is at times focused on military-use IoT systems rather than IoT vulnerabilities research, the inherent challenges of designing secure military-use IoT systems suggest the potential for a high degree of overlap between military-use equipment RD&A and the PLA's operational research into IoT vulnerabilities.

Potentially defensive-oriented military applications for Chinese IoT security research include securing China's "Internet of Underwater Things" and preserving the capabilities of IoT devices in remote military maneuvers far from the Chinese mainland. The imperfect availability of enemy location information in underwater warfare offers a strategic advantage to any nation with advanced underwater sensor technology, and compromised IoT devices and sensor networks operating underwater at a variety of depths could nullify any such advantage. Defense industrial organizations such as Shanghai Jiangnan (Shipyard) Group Ltd. and CSIC's own 722 Research Institute have been supporters of military research into underwater IoT.[581] For its part, the remote operation and defense of IoT networks present similar but distinct challenges that require specialized R&D. Development of IoT technology has the potential to offer the PLA a stronger capability to conduct remote operations, including through the deployment of data-reliant platforms such as UAVs and UUVs, but the tyranny of distance renders sensors far from the Chinese mainland much more difficult to defend and repair in the event of compromise. CASIC's Launch Vehicle Research Design Department in particular has partnered with PLA 63726 Unit on this task.[582]

Intelligence Collection and Network Reconnaissance

A more concerning use of Chinese IoT vulnerability research is to gain unauthorized access to devices and networks for intelligence collection and network reconnaissance purposes. Personnel from several of the PLA's signals intelligence units have published multiple articles on IoT security-related topics, suggesting that these units have likely already exploited device vulnerabilities for these ends. Personnel from the former General Staff Department 3rd Department (总参谋部三部, commonly referred to as 3PLA) responsible for computer network exploitation and signals intelligence are frequent contributors to articles about IoT security vulnerabilities. For

[579] Richard A. Bitzinger, "Civil-Military Integration and Chinese Military Modernization," *China Brief* 4, no. 23, November 24, 2004, https://jamestown.org/program/civil-military-integration-and-chinese-military-modernization/.
[580] Data obtained through searches of the China National Knowledge Infrastructure (CNKI).
[581] "七二二所中标国家物联网应用示范工程" [722 Research Institute Wins Bid for National Internet of Things Application Project] China Shipbuilding Industry Corporation, June 23, 2015, www.csic.com.cn/zgxwzx/zgcydt/307445.htm.
[582] Hao, Ding, Li, and Pang, "Research on Application of Internet of Things in Army Remote Maneuver," 13-14

instance, authors from the 2nd Technical Reconnaissance Bureau (TRB) of the former Lanzhou Military Region, otherwise known as the PLA 69010 Unit,[583] have published extensively on the IoT's ease of attack, specifically enumerating signature emissions from IoT devices as possible avenues for side-channel attacks and listing location tracking features and internet connections as other weak points for exploitation.[584]

Other TRBs subordinated to the former 3PLA have published research that could be useful for targeting more specific IoT devices and applications, ostensibly for intelligence gathering purposes. Personnel from the former Chengdu Military Region 2nd TRB (PLA 78020 Unit)[585] have conducted extensive research on low-duty-cycle wireless sensor networks, a type of network in which sensors mostly remain dormant to conserve power.[586] Past research from authors affiliated with PLA 78020 Unit indicates broader interest in device discovery[587] and specific data transmission error control algorithms,[588] both of which could conceivably be applied in an effort to compromise IoT devices and networks.

Network Attacks and Offensive Information Warfare

The PLA's operational cyber warfare units have also previously shown direct interest in exploiting IoT security vulnerabilities for offensive information warfare. Personnel from the former General Staff Department 4th Department (总参谋部四部, commonly referred to as 4PLA) responsible for offensive cyber operations[589] have published multiple articles on IoT-related topics. For instance, authors from the PLA Electronic Engineering Academy (解放军电子工程学院), a noted

[583] "Project CameraShy: Closing the Aperture on China's Unit 78020," ThreatConnect and Defense Group, Inc., September 24, 2015, https://threatconnect.com/camerashy/.

[584] Yang Ping 杨萍 and Liang Guangming 梁广明, "物联网安全问题及对策分析" [Security Problems and Solutions for the Internet of Things], *无线互联科技 Wireless Internet Technology* 6, (2013): 13.

[585] "Project CameraShy," ThreatConnect and Defense Group, Inc.

[586] Zhenjiang Li, Mo Li, Junliang Li, and Shaojie Tang, "Understanding the Flooding in Low-Duty-Cycle Wireless Sensor Networks," *IEEE Xplore*, 2011 Conference on Parallel Processing, October 17, 2011, https://ieeexplore.ieee.org/document/6047235/.

[587] Chen Liangyin 陈良银, Yan Bingshu 颜秉姝, Zhang Jingyu 张靖宇, Hu Jianbo 胡剑波, Liu Zhenlei 刘振磊, Liu Yan 刘燕, Xu Zhengkun 徐正坤, and Luo Qian 罗谦, "移动低占空比传感网邻居发现算法" (Neighbor Discovery Algorithm in Mobile Low Duty Cycle WSNs), *软件学报 Journal of Software* 25, no. 6, (2014): 1352-1368.

[588] Chen Liangyin 陈良银, Liu Zhenlei 刘振磊, Zou Xun 邹循 et al., "基于能量感知的移动低占空比机会网络纠删编码算法" (Erasure-Coding Algorithm in Mobile Low-Duty-Cycle Opportunistic Networks Based on Energy-Aware), *软件学报 Journal of Software* 24, no. 2, (2013): 230-242.

[589] For more on the roles of 4PLA, see John Costello, "The Strategic Support Force: Update and Overview," *China Brief* 16, no. 19, December 21, 2016, https://jamestown.org/program/strategic-support-force-update-overview/.

former training institute for 4PLA junior officers,[590] have written numerous articles dealing with IoT data collection[591] and cellphone-transmitted viruses.[592]

At least one author from the former 4PLA has written a number of articles directly or indirectly related to the exploitation of IoT security vulnerabilities. One article notes that smart cars are inherently vulnerable to attack: internal car wireless sensor networks, car-mounted controller area network buses, car-mounted local area networking, car software applications, car-mounted onboard diagnostic systems, and smart tire-pressure monitoring systems are specifically identified as components extremely vulnerable to unauthorized access.[593]

Domestic Mass Surveillance

Chinese IoT security research is almost certainly being employed to enhance China's domestic mass surveillance capabilities, namely by research organizations subordinate to China's national police force, the Ministry of Public Security (MPS). Researchers from the MPS's 1st Research Institute (公安部第一研究所) have highlighted the potential of edge IoT computing to manage large amounts of data collected by public security devices as a means of "multi-dimensional prevention and control,"[594] and the MPS 3rd Research Institute hosts an IoT Technology Research Center (物联网技术研发中心) and a penetration testing center.[595]

Evidence indicates that the research elements of the MPS are actively engaged in IoT security research that could likely contribute to unauthorized device access and perhaps offensive exploitation of IoT security vulnerabilities. In 2014, a group of researchers from the MPS's 1st Research Institute conducted a survey of foreign and domestic research into IoT security testing and found that the potentially applicable testing systems were too limited in scope to offer satisfactory active testing tools for IoT security.[596] They highlighted the University of California's SenSec IoT security testing simulation tool; the BANAID test network developed at New South Wales University; the University of Bremen's TAP-SNS simulation and verification testing platform; the Pure Hacking company's research into operational and technological risks associated with RFID systems and their testing of RFID system weak points and vulnerabilities; and the

[590] Mark Stokes, Jenny Lin, and Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," *Project 2049 Occasional Paper,* November 11, 2011, https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/.

[591] Hou Chen 侯琛, Zhao Qianchuan 赵千川, Feng Haoran 冯浩然, Zhang Hao 张浩, and Li Haitao 李海涛, "一种物联网智能数据采集系统的研究与实现" (Research and Implementation of a Kind of Intelligent Data-Collection System in the Internet of Things), *电子测量技术 Electronic Measurement Technology* 37, no. 6, (2014), 108-114.

[592] Liu Guozhao 刘国超, Tan Longdan 谭龙丹, Liu Kesheng 刘克胜, "手机病毒的传播方式及防范研究" (Research on Spread and Prevention of Mobile Phone Virus), *计算机与现代化 Computer and Modernization* 181, (2010), 100-106.

[593] Yang Nan 杨南 and Kang Rongbao 康荣保, "车联网安全威胁分析及防护思路" (Security-Threat Analysis and Defense Strategy of IoV), *通信技术 Communications Technology* 48, no. 12, (December 2015): 1421-1426.

[594] Li Shengguang 李胜广, Li Li 李莉, and Li Gang 李刚, "边缘计算在公安物联网中的应用" [The Application of Edge Computing to Public Security Internet of Things], *中国安防 China Security and Protection* 4, (2018).

[595] "三所简介" [3rd Research Institute Description], Ministry of Public Security 3rd Research Institute, accessed on July 29, 2018, http://hr.trimps.ac.cn/introduction.jhtml/.

[596] Shao Hua 邵华, Li Haitao 李海涛, and Li Chengyuan 李程远, "物联网感知设备安全检测研究" (Research on Security Testing Sensing Equipment of Internet of Things), *信息安全与技术 Information Security and Technology* 2014 (3), no. 243: 23-26, 37.

Tagformance RFID test measurement system created by Finland's Voyantic Ltd. They also acknowledged that Chinese researchers were creating IoT system security simulators and test systems based on the TinyOS simulation system (which was developed as open source software in the United States), and software created by the U.S.-based OPNET Technologies, Inc.[597]

Official statements from Chinese state plans place great prominence on increasing the security of China's IoT ecosystem, but Beijing's support for the IoT security research that undergirds such an effort is an inherently dual-use endeavor that could not only protect Chinese devices from unauthorized access but also enable Chinese government organizations to gain unauthorized access to IoT devices around the world. While the research output of any given Chinese organization seldom constitutes indisputable evidence that it is using IoT security research to enable unauthorized access, the deep civil-military research ties and known missions of prolific military organizations researching IoT security help make the case that Chinese IoT vulnerability research is likely being used to gain unauthorized access to the IoT. Determining specific Chinese intent to use IoT security research to exploit vulnerabilities and gain unauthorized access may be impossible using open source literature, but the existing body of research strongly suggests that the Chinese government has already done exactly that.

Implications for the United States

Securing the IoT from unauthorized access is a daunting task for information security researchers, with the proliferation of attack surfaces and the low barriers to market entry constituting major roadblocks to any such effort. While increased IoT security research is one way to answer these challenges, it is but one tool in the toolbox, and one with significant implications for offensive information warfare.

Meanwhile, China is engaged in a whole-of-nation effort to achieve primacy in IoT security research for reasons of not only economic development but also national security. This approach uses top-level guidance directives to create an ecosystem made up of government funding and institution-building, private sector R&D promotion, and civil-military integration. Just as in a number of critical information technology fields, China feels that the financial costs of these top-down endeavors are outweighed by the long-term strategic, military, and intelligence opportunities that commercial dominance will eventually afford.

Concrete evidence of Chinese government exploitation of IoT vulnerabilities is difficult to find, but Western security researchers have documented at least one notable instance of Chinese exploitation of IoT security vulnerabilities, suggesting that Beijing is prepared to leverage the fruits of its IoT security research ecosystem to advance Chinese national security and economic goals. China's premier civilian intelligence agency, the Ministry of State Security (MSS), appears to have taken a lead in weaponizing IoT exploits for both offensive and espionage operations. One of the most sophisticated botnets targeting IoT devices in recent years has been the "Reaper" botnet, which has exploited vulnerabilities in a wide array of IoT devices in order to link them into a global command-and-control network. Evidence presented in an analysis of the Reaper botnet by Israeli cybersecurity professionals strongly suggests that the Reaper botnet is controlled by an Advanced

[597] Shao, Li, and Li, "Research on Security Testing Sensing Equipment of Internet of Things."

Persistent Threat (APT) actor located within China,[598] and that the group in control of Reaper is the same distinct group that has been identified as "APT18." They have also been referred to by the names "Black Vine," "Deep Panda," and "Axiom" in a number of previous analyses.[599] A number of Western analysts have argued in the past that the threat actor behind APT18, which was also responsible for the 2015 compromise of the U.S. health insurance corporation Anthem, appears most likely to be a unit of the MSS.[600] Such attacks pose a direct threat to sensitive U.S. IoT data even when no Chinese corporate entity is involved in its collection, processing, transmission, or storage.

Chinese exploitation of IoT security vulnerabilities continues apace, even when attacks have not yet been attributed to the Chinese government. The number of attacks originating from China against Finnish IoT devices spiked ahead of the July 2018 meeting in Helsinki between President Trump and Russian President Vladimir Putin.[601] Reports indicate that this recent wave of brute-force attacks was intended to gain access and control over equipment that could collect audio or visual intelligence.[602]

While the above examples are not necessarily representative, they help illustrate some of the implications for the United States. The security vulnerabilities inherent in the IoT may be exploited by an extensive Chinese security research ecosystem to gain unauthorized access to U.S. IoT devices. This type of unauthorized access could have dire national security and economic implications for the United States, ranging from the pilfering of sensitive consumer data, to intelligence targeting of U.S. officials, to a Chinese compromise of critical U.S. infrastructure during crisis or wartime. Any of these consequences could result in significant competitive advantages for Chinese companies or the Chinese government.

[598] Shaun Waterman, "Reaper Authors Chinese, Possibly Linked to Cyberspy Group 'Black Vine,'" *Cyberscoop*, October 30, 2017, https://www.cyberscoop.com/iotroop-reaper-authors-chinese-linked-cyberspy-group-black-vine-anthem-iot/.

[599] "IoTroop Botnet: The Full Investigation," Check Point Software Technologies, October 29, 2017, https://research.checkpoint.com/iotroop-botnet-full-investigation/.

[600] Bill Gertz, "New Chinese Intelligence Unit Linked to Massive Cyber Spying Program," *Washington Free Beacon*, October 31, 2014, http://freebeacon.com/national-security/new-chinese-intelligence-unit-linked-to-massive-cyber-spying-program/.

[601] Sara Boddy and Justin Shattuck, "Cyber Attacks Spike in Finland before Trump-Putin Meeting," *F5 Labs*, July 19, 2018, https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting.

[602] Patrick Tucker, "Chinese Hackers Targeted Internet-of-Things during Trump-Putin Summit," *Defense One*, July 19, 2018, https://www.defenseone.com/technology/2018/07/chinese-hackers-targeted-internet-things-during-trump-putin-summit/149873/.

Recommendations

Although the systemic risk of unauthorized access to IoT devices is not easily mitigated, the increasingly widespread adoption of the IoT and the extent of Chinese IoT vulnerability research call for more rigorous policy measures to better secure the IoT from unauthorized access. These recommendations fall into two main categories.

Improving Overall IoT Security

1. Encourage adoption of security best practices for IoT products in the form of an industry-backed cybersecurity program.

IoT security vulnerabilities remain difficult to understand at a glance for the lay consumer, and the IoT industry lacks incentives to emphasize security best practices in IoT products. This contributes to weakened overall security for IoT devices. An industry-backed cybersecurity program or certification could create market incentives for companies to adopt a set of security best practices in a manner easily understood by U.S. consumers, especially given the potential harm that could occur and the relative inability of the average consumer to protect themselves from unauthorized access. These security practices could be vetted by both government agencies[603] and independent NGOs, and may include penetration testing, automated software and firmware updates, encrypted communication, unique device identification credentials, and redundant functionality in case of connectivity failures, among other features. Products that comply with these best practices could carry a "Secure IoT Device" logo or notation, analogous to the EnergyStar program, that would create product differentiation in a crowded market for IoT devices.[604]

2. Increase funding and support for IoT security research, especially in areas that could yield proportionately greater gains for IoT security.

Increased funding for IoT security research in selected fields could yield significant gains for IoT security. For instance, fog computing, or the deployment of cloud computing resources closer to endpoint IoT devices on the edges of networks, could significantly enhance IoT device security by funneling computing resources to smaller, mobile IoT devices with limited onboard security capability.[605] Better AI algorithms that recognize anomalous behavior consistent with unauthorized access to IoT devices could become a first-line security measure for handling the massive amounts of data and traffic that result from widespread IoT adoption. Increased funding in these fields funneled to academic; corporate; and independent, non-corporate organizations could greatly accelerate the deployment of more effective IoT security practices.

[603] Some U.S. government agencies have already issued documents recommending security best practices, namely the "Strategic Principles for Securing the Internet of Things," United States Department of Homeland Security, November 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.

[604] "Internet of Things (IoT) Security and Privacy Recommendations," Broadband Internet Technical Advisory Group, November 2016, http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf.

[605] Chiang, Balasubramanian, and Bonomi, *Fog for 5G and IoT*, 261-281.

Risks of Chinese Exploitation of IoT Security Vulnerabilities

1. *Document Chinese entities that conduct IoT security research for, alongside, and supported by the Chinese military and security services.*

A large share of Chinese civilian and commercial research entities focused on IoT development have connections to China's government, military, and security apparatuses. Given the dual-use nature of IoT security vulnerability research, formal documentation of these Chinese entities is an important first step in forestalling the offensive use of IoT security research to gain unauthorized access to U.S. IoT devices. Once a list of these entities is established, higher-level decisions regarding how to treat entities on this list can be made, possibly including restrictions on cooperation with these entities.

2. Overhaul the oversight process for green-lighting Chinese investment in the U.S. IoT industry in order to better account for the unique security concerns posed by China's blending of its military and civilian IoT research ecosystems.

China's blending of its military and civilian IoT research ecosystems amplifies concerns about Chinese technology transfer efforts and supply chain integrity. Enlarged Chinese investment presence in U.S. IoT companies may warrant further scrutiny, especially since the research and intellectual property of these companies may become subject to Chinese technology transfer efforts that wind up aiding Chinese companies or military modernization efforts. Chinese investment in U.S. IoT manufacturers may also compromise the U.S. IoT supply chain for critical infrastructure and military applications. New legislation like the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) strengthens the authority and ability of existing U.S. government organizations like CFIUS to review potentially risky inbound Chinese investments, but these regulatory bodies should be especially cautious of investments in U.S. IoT suppliers and block transactions that may jeopardize U.S. national security.

Chapter 4: Authorized Access and Privacy Risks to U.S. Citizens from Chinese Data Access

While technical vulnerabilities that enable unauthorized access to IoT devices are numerous, even authorized access to these devices may reveal large amounts of sensitive data on U.S. citizens. Because unauthorized back-door access to IoT devices has received the lion's share of research attention, however, the reach and implications of authorized data access from IoT devices remain comparatively understudied. Authorized access to IoT data, defined here as information access permitted or not specifically forbidden by the end user, enumerated by corporate agreement, or enshrined in legal statute, is closely related to a user's privacy, used here to mean the right or ability to control disclosure of information.[606] While the previous section detailed various potential unauthorized means of data access and their impact on the security of the IoT, especially for U.S. consumers, authorized data collection can tap into a wide variety of information with substantial impact on a user's privacy, often with the user's consent, if not their explicit awareness or understanding.

Authorized data access is an indispensable part of the IoT's transformative potential. The massive amounts of data obtained by IoT devices through authorized access constitute a substantial economic and strategic advantage. Like many of their non-Chinese competitors, Chinese IoT companies are collecting extensive amounts of information through various conduits for competitive business advantage. Many of these ongoing data collection efforts are not expressly authorized, and thus undertaken without the user's specific consent, though the activity may be legal and permitted under current regulations.

The increasing Chinese presence in the U.S. IoT market means that the amount of information Chinese IoT products collect and make available to Chinese entities is expanding. Chinese access to U.S. IoT data is inextricably linked to the overall privacy of IoT users, as well as the economic and national security interests of the United States. This raises several important questions: To what degree are Chinese companies and the Chinese government able to access information collected from U.S. IoT users, and what types of information are they able to obtain? What are the implications and purposes of this data acquisition, and what can and should be done about it?

U.S. citizens who use Chinese IoT devices may find their data accessed through a variety of authorized avenues. The first means of access includes authorized (or at least not expressly forbidden) conduits common to many IoT devices and companies around the world. More concerning, however, are China's uniquely sweeping legal statutes that could enable the Chinese government to access U.S. IoT data stored in or transmitted to China, and potentially exploit it for economic and national security advantages.

The United States' complex tapestry of laws and guidelines are at present insufficient to the task of protecting U.S. IoT data from this range of threats to privacy. As discussed below, new policy approaches are necessary in order to both safeguard existing protections and expand them to meet the growing privacy needs of U.S. consumers.

[606] Many information security specialists regard "privacy" as the assurance of confidentiality, while "security" is a set of measures meant to protect privacy. For a more thorough treatment of the distinction, see Houbing Song, Glenn A. Fink, and Sabina Jeschke, eds., *Security and Privacy in Cyber-Physical Systems* (Hoboken, NJ: Wiley-IEEE Press, 2017), 1-3.

Chinese Access to U.S. IoT Data

Chinese companies and government entities can obtain U.S. IoT data through a variety of means, even without resorting to the kind of unauthorized access as discussed in Chapter 3. These methods can be grouped into general levels of access–user, device, corporate, and those granted by the Chinese law–with each successive level being comparatively less transparent to average IoT users and offering a greater degree of bulk access to U.S. IoT data. While many authorized data access methods are common across the entire IoT and are not necessarily unique to Chinese products or companies, the most substantive threat to U.S. privacy hinges on the behavior of the Chinese government, which is uniquely empowered to access U.S. IoT data well in excess of the international norm.

At the user-level, Chinese entities could access U.S. data simply from sales and usage of their IoT products by U.S. consumers who authorized data collection and transmission, either knowingly or unknowingly, by agreeing to terms of use. Both empirical and anecdotal studies have found that many users pay little attention to application permissions or end user license agreements that authorize data collection and detail user rights.[607] End user license agreements and data permission notifications arguably remain the most transparent form of data access for IoT users, who are in theory notified of data collection and future usage.

Data access at the device level is typically more opaque to the end user. Access through the device manufacturing and design process opens up opportunities for outside entities to collect even more information at scale than authorized access through any individual end user's device. Chinese entities may be able to access U.S. data in situations where U.S. IoT companies source hardware or software components from China that transmit user data abroad–as was the case in 2017, when smart doorbells with Chinese components were discovered to be unintentionally sending audio data to Chinese servers.[608] Chinese companies building IoT infrastructure, especially those firms leading the charge on 5G deployment, can also potentially access U.S. data by capturing, monitoring, and storing IoT data that passes over networks using their equipment. Access through these conduits could collect data not only from IoT devices with Chinese components, but also from all devices connected to networks with Chinese hardware and software. Data access through manufacture and design is not transparent for the average IoT consumer, requiring deep knowledge of the specific hardware and software to even be aware that a foreign entity is obtaining data.

Corporate-level data access enables Chinese entities to access U.S. IoT data at an even greater scale. This can occur through a variety of avenues. Chinese companies could buy U.S. IoT companies and the data they have accumulated through their products, or more simply, Chinese firms could buy U.S. data through a third-party vendor or a data broker. In China, joint venture agreements between U.S. IoT firms and their Chinese counterparts could result in the sharing of

[607] For an empirical example, see Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior* (Technical Report No. UCB/EECS-2012-26) (Berkeley, CA: University of California at Berkeley, 2012), accessed May 2, 2018, https://www2.eecs.berkeley.edu/Pubs/TechRpts/2012/EECS-2012-26.pdf; for an anecdotal study, see Catharine Smith, "7,500 Online Shoppers Accidentally Sold Their Souls to Gamestation," *Huffington Post*, June 17, 2010, https://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html.

[608] Aaron Tilley, "This Smart Doorbell Was Accidentally Sending Data to China, Until People Started Freaking Out," *Forbes*, March 22, 2017, https://www.forbes.com/sites/aarontilley/2017/03/22/this-smart-doorbell-was-accidentally-sending-data-to-china-until-people-started-freaking-out/#1d029f3b5984.

collected user data between the United States and the Chinese partner. Corporate-level data access may be even more opaque than the previous two conduits, especially when protected from disclosure to end users or the general public by non-disclosure agreements or corporate legal statutes.

Sitting atop all of these means of data access and transfer are the broad data appropriation powers that Chinese law accords to Chinese government authorities. Powers wielded by nation-states provide the most wide-ranging potential for access to U.S. data. For instance, Chinese data storage companies holding U.S. IoT data could be compelled to hand over this information to government authorities, and U.S. IoT companies operating in China could likewise face strong pressure from the Chinese government to hand over U.S. data. Existing Chinese legal statutes apply to all Chinese companies and are broad enough to suggest that the Chinese government could compel access to U.S. IoT data through legal channels at the user, device, and corporate levels, even outside of Chinese borders. Any Chinese government access to U.S. data is likely to be carried out discreetly in order to avoid any compromise of Beijing's motives or international uproar, rendering this form of data access the most opaque of the methods discussed here.

While the examples described above may not constitute an exhaustive accounting of the types of authorized data acquisition, most forms of data acquisition would fall into these main categories. The remainder of this chapter addresses which of these methods of data access constitute the greatest challenges to U.S. IoT data privacy, and what can be done to address these threats.

An Assessment of Authorized Data Access Methods

Which types of authorized data access methods present the greatest risks to U.S. IoT data privacy, and which ones are materially less concerning? Broadly speaking, the amount of information on a user that may be obtained (depth) and how many users' data may be acquired (scale) are two main determinants of the amount of risk to U.S. data privacy. Because these factors can ultimately prove difficult to assess quantitatively and mean little when examined without context, this chapter describes the occurrence of these factors in the various means of authorized data access by examining a variety of qualitative examples across the various types of data access methods identified above. The following sections detail these examples with a specific focus on Chinese access to U.S. IoT data.

User-Level Data Access

Authorized data access at the user-level is typically disclosed in two main ways for consumer IoT products. The first, governing information collected by IoT hardware and its directly associated software, is through the terms and conditions that are agreed to when a user consents to a product's End User License Agreement (EULAs), terms of service, and broader privacy policies after purchasing and using an IoT device for the first time. The second is through application-specific permissions that users are notified of when running software that manages their IoT device, which ultimately collects information on a user's IoT device controller like a smartphone, computer, or tablet.

Data Access According to EULAs, Terms of Service, and Privacy Policies

An examination of selected Chinese EULAs, terms of service, and privacy policies suggests that much of the substantive data collected by Chinese IoT devices is generally comparable to the types and scope of data collected by U.S. IoT devices.

A small-scale survey of several Chinese-based IoT companies suggests that it is uncommon for Chinese-based IoT firms to post full versions of their EULA agreements online. Of the ten Chinese-based firms selling home appliance IoT devices and involved in IoT production listed in the business-to-business database IoT One, only one had a full EULA text for its devices available on its website.[609] That firm, Huawei Technologies Company, Ltd. (华为技术有限公司), was by far the largest of the companies listed, and maintains the largest global footprint.

At least some of the data collection provisions of the general Huawei EULA appear to be consistent with policies used by some U.S. firms. For instance, Huawei notes that "its affiliates/licensors may collect data from your device for analysis. Collected data includes your device configuration data, application statistical data, and error log data. All data is anonymized before being collected and processed."[610] This language is similar to wording found in Apple's standard EULA for Mac applications, for instance, which states that Apple "may collect and use technical data and related information—including but not limited to technical information about your device, system and application software, and peripherals... [Apple] may use this information, as long as it is in a form that does not personally identify you, to improve its products or to provide services or technologies to you."[611]

Privacy policies for several major Chinese IoT companies with operations or products in the United States offer further details on the types of information collected at the user-level. For instance, Huawei's privacy policy states that it may collect personal data volunteered by the user, device and application information, mobile network information, log information, location information, any information the user stores on Huawei cloud servers, and information from third party sources.[612] Many of these practices are typical for the industry.

Other major Chinese IoT companies make similar disclosures. Privately-owned Xiaomi is the world's fourth largest smartphone manufacturer and one of the largest suppliers of mobile devices and wearable technology in China alongside Huawei, Vivo, and Oppo.[613] Xiaomi notes in its privacy policy that its devices may collect all information uploaded voluntarily by the user, device or SIM-related information, location information, and log information.[614] Xiaomi is not typically

[609] "HQ Countries," IoT One, accessed May 12, 2018 https://www.iotone.com/vendor/searchlist?filterName=Industry&HQCountry=CN&Industry=10&FunctionalArea=&Capability=&HardwareDigest=&SoftwareDigest=&ServicesDigest=&ConnectivityProtocols=&Revenue=&UseCase=&R_Industry=OR&R_FunctionalArea=OR&R_UseCase=OR&R_HardwareDigest=OR&R_SoftwareDigest=OR&R_ServicesDigest=OR&R_ConnectivityProtocols=OR&vendorSort=RankScore%20DESC,%20NameSort%20ASC,%20IoTSnapshotCount%20DESC&order=DESC.

[610] "End-User License Agreement," Huawei, Inc., accessed May 15, 2018, https://consumer.huawei.com/en/legal/eula/. This EULA is described as an "End-User Software Licensing Agreement" that is applicable "for part of Huawei's consumer products, including without limitation phone and tablet, etc. [sic]." See "Legal," Huawei, Inc., accessed May 15, 2018, https://consumer.huawei.com/en/legal/.

[611] "Licensed Application End User License Agreement," Apple, Inc., accessed May 15, 2018, https://www.apple.com/legal/macapps/stdeula/.

[612] "Huawei Consumer Business Privacy Statement," Huawei, Inc., April 15, 2018, accessed May 15, 2018, https://consumer.huawei.com/en/legal/privacy-policy/.

[613] Manya Koetse, "Top 10 Most Popular Smartphones in China 2017 (According to Weibo)," *What's on Weibo,* November 1, 2017, https://www.whatsonweibo.com/top-10-popular-smartphone-brands-china-2017-according-weibo/; James Yan, "China Smartphone Market 2017: Top 10 Best-Selling Models," *Counterpoint Research,* January 15, 2018, https://www.counterpointresearch.com/china-smartphone-market-2017-top-10-hot-sale-models/.

[614] "Privacy Policy," Xiaomi, Inc., updated May 25, 2018, accessed October 23, 2018, http://www.miui.com/res/doc/privacy/en.html.

identified as a major Chinese IoT participant in the U.S. market because its devices are not yet directly sold in the United States,[615] but the firm offers a wide variety of IoT products, including air purifiers, temperature sensors, lighting fixtures, and other appliances.[616] The firm is poised to start selling IoT devices on the U.S. market as soon as late 2018,[617] and many smart devices offered by Xiaomi such as speakers, power banks, and "Mi Box" TV support tools are already available to U.S. consumers through large retailers like Walmart.[618]

Much of the information collection and access disclosed in Chinese IoT privacy policies is nearly identical to that collected by U.S. IoT companies. Google's privacy policy, for instance, discloses nearly identical categories of information collection,[619] and Apple's privacy policy describes similar types of personal information collection.[620]

Other data access provisions in Chinese IoT privacy policies and EULAs, however, may represent significant departures from corresponding U.S. provisions. For instance, one important data access disclosure notes that Huawei may transfer collected data outside of the country where the user resides. Huawei's general EULA expressly states that

> *"…all data collected from your device may be processed or transferred to Huawei and its affiliates/licensors in countries outside of the country you reside [sic].* ***This means the data may be transferred to or accessed from other jurisdictions which are outside of the country where you use Huawei's products or services*** *[emphasis added]***.** *These jurisdictions may have different data protection laws, or such laws may not even exist. In such cases, Huawei will ensure that a similar and adequate level of protection is afforded to the data as required by all applicable laws and regulations."*[621]

Comparable Apple EULAs make no such disclosure, and no similar disclosures were found in product-specific EULAs for IoT products like the Apple HomePod smart speaker.[622] Manufacturers may still make such data transfers, but doing so without disclosing them would likely expose a company to legal or other serious public repercussions.

[615] Liza Lin and Dan Strumpf, "Xiaomi Set to Enter U.S. Smartphone Market as Early as This Year," *Wall Street Journal*, March 5, 2018, https://www.wsj.com/articles/xiaomi-set-to-enter-u-s-smartphone-market-as-early-as-this-year-1520235047.

[616] A full list of devices is available from "Smart Devices," Xiaomi, Inc., accessed May 15, 2018, https://xiaomi-mi.com/mi-smart-home/.

[617] Lin and Strumpf, "Xiaomi Set to Enter U.S. Smartphone Market as Early as This Year"; Jon Russel, "Xiaomi is Bringing its Smart Home Devices to the US- but Still No Phones Yet," *Techcrunch*, May 10, 2018, https://techcrunch.com/2018/05/10/xiaomi-is-bringing-its-smart-home-devices-to-the-us-but-still-no-phones-yet/.

[618] Micah Singleton, "Xiaomi's 4K Mi Box is Officially on Sale in the US," *The Verge*, April 20, 2018, https://www.theverge.com/circuitbreaker/2016/10/3/13150534/xiaomi-4k-mi-box-us-release-sale.

[619] "Welcome to the Google Privacy Policy," Google LLC, updated December 18, 2017, accessed May 15, 2018, https://policies.google.com/privacy?hl=en-us#infocollect.

[620] "Privacy Policy," Apple, Inc., updated January 19, 2018, accessed May 15, 2018, https://www.apple.com/legal/privacy/en-ww/.

[621] "End-User License Agreement," Huawei, Inc.

[622] See "Licensed Application End User License Agreement," Apple, Inc., accessed May 15, 2018, https://www.apple.com/legal/macapps/stdeula/ and "Apple HomePod Software License Agreement," Apple, Inc., accessed May 15, 2018, https://www.apple.com/legal/sla/docs/HomePod.pdf.

Other EULAs for Chinese IoT products appear to reserve the right to preserve information for transfer to government authorities. Xiaomi's general EULA notes that the company can "…[save] relative information [sic] and [report] to relevant authorities based on the applicable laws and regulations."[623] The company's U.S. privacy policy notes that the company can transfer personal information outside of the user's jurisdiction "in accordance with applicable laws,"[624] a vague statement that does not rule out compliance with Chinese laws even if accepted practice holds that the company must abide by the laws of the country where the product is used. Further, the company reserves the right to store data from the United States in its overseas data centers, including its site in Beijing.[625]

Specific references to overseas data transfer aside, however, some of the language in Chinese IoT privacy policies is substantively similar to wording used by U.S. IoT companies. Both Chinese and U.S. IoT companies include provisions for cooperation with government entities, where disclosures for Chinese IoT products generally bear closer resemblance to U.S. privacy policies across the board. A comparison of the provisions employed by Chinese and U.S. IoT companies is available in the table below.

Table 8: Privacy Policy Text Regarding Cooperation with Government Entities

Apple	Google	Huawei
Can disclose user information if required to by "law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence" [626]	May disclose data to "meet any applicable law, regulation, legal process or enforceable governmental request" [627]	May share user information "when there is a reasonable requirement to do so, for example, to meet request of applicable law, regulation, legal process or enforceable government [sic]" [628]

The cases described above are neither exhaustive nor comprehensive documentations of the types of data collection and access at the user-level, but instead help describe the types of data collection and access specified in end user license agreements, privacy policies, and terms of service, especially for IoT products from Huawei and Xiaomi, two of the largest IoT companies in China and in the world. More information on types of data collected by IoT devices at the user-level can be found by examining application permissions granted to IoT device controllers like smartphones, computers, and tablets.

Data Access According to Application Permissions

In addition to data gathered from IoT hardware disclosed by company privacy policies, the applications used to control those devices can also act as conduits for data collection. Home

[623] "Xiaomi User Agreement," Xiaomi, Inc., accessed May 15, 2018, http://www.miui.com/res/doc/eula/en.html.
[624] "Privacy Policy," Xiaomi, Inc., updated May 6, 2016, accessed May 13, 2018, http://www.mi.com/en/privacy/.
[625] Ibid.
[626] "Privacy Policy," Apple Inc.
[627] "Welcome to the Google Privacy Policy," Google LLC.
[628] "Huawei Consumer Business Privacy Statement," Huawei Technologies Co., accessed May 14, 2018 https://consumer.huawei.com/en/legal/privacy-policy/.

management devices such as the Amazon Echo and Google Home smart speakers are controlled through associated applications (e.g., Amazon Alexa and Google Home) that are installed on the user's smartphone or tablet device. In order to use the network function of a product, the user generally has to grant permission for said application to access portions of their personal data.[629]

Most of this access is fairly benign. For example, a smartphone application may request details about a person's location in order to give accurate details about local weather conditions.[630] Nevertheless, enabling these programs can reveal extensive and intimate details about a given person. These device control apps generally require the granting of extensive permissions in order to function and could potentially collect extensive profiles on a person's communication habits and device usage.

Chinese IoT products, like their U.S. counterparts, are often managed by downloadable applications. For instance, Xiaomi IoT products can be managed via an application that is downloaded onto the owner's smartphone or tablet device. The "MiHome" application is available from the Apple App Store and Google Play. Like other home applications, the MiHome app can access numerous functions of the user's phone or tablet if given user permission. These permissions include abilities to read a user's phone contacts, send and receive text messages, use GPS for location, take photos and videos, record audio, and more.[631] A full comparison of the MiHome application's accessible permissions and those of comparable applications like the Google Home and Amazon Alexa application is available in Appendix A.

Negative consumer feedback about Xiaomi's MiHome application suggests a perception that the company's data collection may be overly intrusive. Several consumer reviews of the Xiaomi app criticized it for giving overly broad permissions. For example, one user criticized the MiHome app for having "ridiculously abusive" permissions, such as potentially being able to log what calls have been made on the user's device, what logs the phone downloads, and what external apps are available on it.[632] Comparisons available in Appendix A however, suggest that the MiHome app's required permissions are broad but roughly comparable to those granted to similar products from competitors.

Some of the negative perception surrounding Xiaomi's intrusiveness may be attributable to past accusations of impropriety with user data. In 2014, a report by the firm F-Secure found that Xiaomi phones being sold outside of China were secretly sending user data such as SMS files back to servers based in China.[633] This alert prompted India's Air Force to warn its personnel that certain Xiaomi-brand phones may be a security risk.[634] Taiwan's National Communications Commission (國家通訊傳播委員會) also launched a probe to investigate if Xiaomi had breached data

[629] Chris Hoffman, "How Android App Permissions Work and Why You Should Care," *MakeUseOf*, May 21, 2012, https://www.makeuseof.com/tag/app-permissions-work-care-android/.

[630] "About Privacy and Location Services in iOS 8 and Later," Apple Inc., accessed May 12, 2018, https://support.apple.com/en-au/HT203033.

[631] "MiHome" App Page, Google Play App Store, accessed May 12, 2018, https://play.google.com/store/apps/details?id=com.xiaomi.smarthome&hl=en.

[632] Ibid.

[633] Hugo Bara, "Testing the Xiaomi RedMi 1S," *F-Secure Labs*, August 7, 2014, https://www.f-secure.com/weblog/archives/00002731.html.

[634] NDTV, "Indian Air Force Asks Personnel Not to Use Chinese Xiaomi Phones," *NDTV*, October 24, 2014, https://www.ndtv.com/india-news/indian-air-force-asks-personnel-not-to-use-chinese-xiaomi-phones-683720.

protection laws, but the probe eventually concluded that the firm had not violated said laws.[635] Nonetheless, Xiaomi moved to counter these accusations over data privacy by announcing that it would be shifting data storage for international customers to Amazon AWS data centers in Oregon and Singapore.[636] Xiaomi continues to draw fire in spite of these measures, most recently for altering its privacy policy for devices in the United States[637] to enable them to collect information on the user's employer, job status, passport information, IMEI number, location, log and app information.[638]

Overall, Chinese data access at the user-level, as disclosed in privacy policies and application permissions, is something of a mixed bag. Much of the information collected by Chinese IoT devices from two of the largest Chinese IoT companies, Huawei and Xiaomi, is not necessarily substantially different from data collected by U.S. IoT devices, but the privacy policies and EULAs of these two companies appear to leave significant leeway for overseas transfer and storage of data collected at the user-level. While information from two Chinese IoT companies is hardly a representative sample, the size and reach of Huawei and Xiaomi's privacy policies and application permissions are bound to have a notable effect on U.S. consumers.

Device-Level Data Access

At the device-level, the sub-components that allow IoT devices to function could also act as conduits through which data can be transmitted to an offshore entity. Because existing standards governing who owns and controls data generated by IoT devices are extremely ill-defined,[639] numerous entities could conceivably claim ownership over the data generated by a device, including the device manufacturer, the producer of the sensors that went into the device, or the end user themselves. Consequently, experts agree that any one of these actors could claim that they are legally permitted to gather data from the devices that they help to manufacture, thereby opening another route through which Chinese entities could access U.S. IoT data.[640]

Despite the possibility of this type of device-level data access, very little information currently exists on whether Chinese sensor components actually gather data from their host devices and whether or not this type of access would be outside of accepted practice around the globe. Given the unresolved ownership status of data collected and the potential case for data ownership by sub-component manufacturers and other third parties, a user would need to conduct a thorough technical inspection of the IoT device to ascertain if it is sending data to foreign-owned servers, making the lack of direct evidence supporting this type of data access unsurprising. Several Western government and intelligences agencies have prohibited the use of Chinese information

[635] Wang Maozhen 王茂臻, "NCC：抽測陸手機 資安無虞" [NCC: Selected Testing of Chinese Cellphones Reveal No Data Security Concerns], *聯合日報 United Daily News*, December 30, 2014, https://udn.com/news/story/7098/611665.

[636] Andy Boxall, "To Help Quell Privacy Fears, Xiaomi Shifts Its International Data Storage Out of China, *Digital Trends*, October 23, 2014, https://www.digitaltrends.com/mobile/xiaomi-shifts-data-storage-china/.

[637] Debashis Sarkar, "New Xiaomi Privacy Policy Will Collect Users' Personal Info, Financial Details, and More," *Gadgets Now*, May 4, 2018, https://www.gadgetsnow.com/tech-news/new-xiaomi-us-privacy-policy-will-collect-users-personal-info-financial-details-and-more/articleshow/64026044.cms.

[638] "Privacy Policy," Xiaomi Inc., accessed May 11, 2018, http://www.mi.com/us/about/new-privacy/.

[639] David Wallace, "Who Owns the Data in the Internet of Things," *PTC*, accessed May 12, 2018, https://www.ptc.com/en/product-lifecycle-report/who-owns-the-data-in-the-internet-of-things.

[640] Barb Darrow, "The Question of Who Owns the Data is About to Get a Lot Trickier," *Fortune,* April 6, 2016, http://fortune.com/2016/04/06/who-owns-the-data/.

technology hardware over concerns about device-level backdoors,[641] and one well-sourced China watcher has remarked that Chinese engineers who have experience with Huawei have confirmed that the company installs backdoors in its products.[642] In October 2018, reports emerged that a PLA unit had installed Chinese hardware implants in U.S. devices in what officials called "the most significant supply chain attack known to have been carried out against American companies."[643] Still, concrete open source evidence on what kind of backdoors and what types of data they would exfiltrate remains difficult to come by, and the reports of PLA hardware implants have been contested by several parties.[644] Device-level data access merits further examination, especially given the multiple potential conduits for transfer of U.S. IoT data to Chinese entities.

IoT infrastructure is comprised of thousands of devices ranging from automobiles to appliances to manufacturing implements.[645] Data generated by these devices is collected and analyzed in bulk in order to derive benefit from network-enabled devices. For example, a municipal power company may use cloud computing to store thermostat data from its consumer base, and then send that data back to consumers to enable them to allocate power more efficiently. Data collected by IoT devices generally passes through four stages:[646]

1) *Collection*: Data is collected via a sensor or actuator such an infrared detector, pressure sensor, or proximity sensor.
2) *Aggregation*: the collected data is aggregated and converted into digital streams via data acquisition systems (DAS). It can then be routed to a central server or cloud system.
3) *Pre-processing*: As an optional step, data acquired by IoT systems can be processed via an edge IT system to make sure that it is more manageable and ensure that no information is lost during transfer to storage.
4) *Cloud storage*: Data is forwarded to a physical data system or cloud-based system, where data can be stored and analyzed to produce results.

Of these steps, the collection, aggregation, and cloud storage components represent stages in which user data could be routed to offshore servers.

<u>Collection</u>

China possesses an extremely robust production capacity for IoT device components, especially in sensors and actuators. Consequently, Chinese-brand sensors and actuators, which are frequently used in U.S. IoT products, may open possible routes for collecting diagnostic data that could ultimately wind up in the hands of Chinese entities, in much the same way data could wind up in

[641] Adi Robertson, "Lenovo Reportedly Banned by MI6, CIA, and Other Spy Agencies Over Fear of Chinese Hacking," *The Verge*, July 30, 2013, https://www.theverge.com/2013/7/30/4570780/lenovo-reportedly-banned-by-mi6-cia-over-chinese-hacking-fears.

[642] Bill Bishop, Twitter post, April 28, 2018, https://mobile.twitter.com/niubi/status/990358142952394752.

[643] Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg,* October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[644] Jordan Robertson and Michael Riley, "The Big Hack: Statements from Amazon, Apple, Supermicro, and the Chinese Government," *Bloomberg,* October 4, 2018, https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond.

[645] "Overview of Internet of Things," Google Inc., accessed May 12, 2018, https://cloud.google.com/solutions/iot-overview.

[646] JR Fuller, "The 4 Stages of an IoT Architecture," *TechBeacon*, accessed May 12, 2018, https://techbeacon.com/4-stages-iot-architecture.

the hands of any original equipment manufacturer.[647] For example, Shanghai Fudan Microelectronics Company (上海复旦微电子集团股份有限公司), known as Fudan Micro, is a major producer of sensor and actuator technology that also maintains a patent presence in the United States.[648] The firm produces a variety of components parts used in security, identification, and payment technologies, including microprocessors, electrically erasable programmable read-only memory (EEPROM) products, and CPU cards for contactless readers.[649] Fudan Micro is listed as one of the top suppliers by market share in the U.S. market for IC Card Chip Technology, alongside Qualcomm, Apple, and IBM.[650] It also owns R&D institutes in the United States, as well as offices in Taiwan, Singapore, and San Jose.[651] While no available evidence suggests that U.S. IoT data is being collected by Shanghai Fudan, the importance of field-collected data to its R&D efforts in the United States could justify data collection from U.S. IoT devices that contain Shanghai Fudan components. Additionally, given that Fudan Micro focuses on products that deal with personally identifiable information and security maintenance, it is possible that the sensors that they manufacture could log sensitive financial or security-related data.

Some Chinese sensor manufacturers have also directly partnered with U.S. firms in order to analyse their consumer base, opening another potential conduit for access to U.S. IoT data. In 2017 the Shenzhen-based firm GZTech Group (广众通电子 (深圳)有限公司), a hardware and firmware developer that supports IoT services, partnered with the clothing firm American Eagle to analyze how customers interact with the layout of their stores.[652] The project was implemented as a trial in flagship American Eagle stores in Shanghai and Hong Kong.[653] It is unclear whether the program will be extended to other American Eagle locations across the world. Although there is no direct evidence identifying who collects and stores the information, the collected information may eventually wind up in the possession of the GZTech Group.

[647] Katerina Megas, Ben Piccarreta, and Danna Gabel O'Rourke, eds., "Internet of Things (IoT) Cybersecurity Colloquium: A NIST Workshop Proceedings," National Institute of Standards and Technology, December 2017, https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8201.pdf.

[648] "上海复旦微电子集团股份有限公司" [Shanghai Fudan Microelectronics Group Co., Ltd.], 摩尔精英网络科技南京有限公司 Moore Network Technology Co. Ltd, accessed May 13, 2018, http://www.moore.ren/company/detail.htm?companyId=110584; "公司介绍" [Company Profile], 上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Co., accessed May 13, 2018 http://www.fmsh.com/about.shtml.

[649] "产品" (Products and Solutions), 上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group o., accessed May 14, 2018 http://www.fmsh.com/products.shtml.

[650] "United States IC Card Chip Market Report 2017," Decisions Database, accessed May 14, 2018, http://www.decisiondatabases.com/ip/897-united-states-ic-card-chip-industry-market-report.

[651]"上海复旦微电子集团股份有限公司" [Shanghai Fudan Microelectronics Group Co., Ltd.], 摩尔精英网络科技南京有限公司 Moore Network Technology Co. Ltd, accessed May 13, 2018, http://www.moore.ren/company/detail.htm?companyId=110584; "公司介绍" [Company Profile], 上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Co., accessed May 13, 2018 http://www.fmsh.com/about.shtml.

[652] The partnership was done through one of GZTech's subsidiaries, FlyingCodes. See GZTech Group, "FlyingCodes 新一代有礼•指 2.0 助力美国一线服装品牌 "American Eagle"进行店铺客流及客流店铺行为分析" [FlyingCodes Helps Major American Clothing Brand "American Eagle" Analyze Customer Flow], *GZTech Group*, August 28, 2017, http://www.gztechgroup.com/index.php?id=52.

[653] GZTech Group, "FlyingCodes 新一代有礼•指 2.0 助力美国一线服装品牌 "American Eagle"进行店铺客流及客流店铺行为分析" [FlyingCodes Helps Major American Clothing Brand "American Eagle" Analyze Customer Flow], *GZTech Group*, August 28, 2017, http://www.gztechgroup.com/index.php?id=52.

Data Aggregation

While it is theoretically possible for a device to route data packets to offshore servers, there have yet to be any reported incidents of this occurring. The exact means by which data is aggregated and transmitted on Chinese IoT device components varies depending on manufacturer standards. However, broadly speaking, Chinese device manufacturers use the same tools and methods as their Western counterparts when gathering and managing the flow of data from multiple devices. For example, a device in China would convert analog data gathered from sensors to digital streams using a sampling controller.[654] These data packets would then be sent to a host server,[655] and these data packets could then be analysed using common data management tools such as Apache Hadoop.[656] Once the data is aggregated, the destination of the packets is dependent on the manufacturer, which is more likely to be located in China than in other countries given China's massive technology manufacturing footprint.

Cloud Infrastructure

A third potential point of device-level data access is rooted in cloud storage and computing—essential for storing and processing IoT data—where Chinese software providers are playing an increasingly prominent role. Foremost among these is Alibaba Group Holding Ltd. (阿里巴巴集团控股有限公司), which maintains a robust cloud computing service.[657] In March 2018, Hu Xiaoming, president of Alibaba's cloud computing division, announced that the firm considers IoT to be a major "strategic track," and that it intends to build a market of over 10 billion connected IoT devices in the near future.[658] It is conceivable that Alibaba could come to compete with services like AWS for a share of the U.S. data market, including the data stored by IoT devices. According to company policy, Alibaba's data centers are situated locally in various focal point countries, rather than having their servers located in China.[659] However, it is worth noting that according to Alibaba's privacy policy, it would be required to transfer data to government entities if required to by "law, legal process or lawful government request."[660]

An overall examination of Chinese device-level access to U.S. IoT data reveals that this type of data access is not only understudied but also likely underreported. Nevertheless, the unresolved legal status of data ownership coupled with increasing Chinese presence in device manufacturing

[654] Wu Zhongjie, "物联网硬件：网络化数据采集系统" [Internet of Things Hardware: Networked Data Acquisition System], *51CTO,* May 28, 2014, http://blog.51cto.com/alanwu/1418150.

[655] Wu, "Internet of Things Hardware: Networked Data Acquisition System."

[656] tom_fans (username), "物联网数据采集处理架构" [Internet of Things Data Acquisition and Processing Architecture], *CDSN*, November 11, 2017, https://blog.csdn.net/tom_fans/article/details/78667779.

[657] Ron Miller, "Alibaba Cloud Growing like Gangbusters, But Still Far behind AWS and Other Market Leaders," *TechCrunch*, February 6, 2018, https://techcrunch.com/2018/02/06/alibaba-cloud-growing-like-gangbusters-but-still-far-behind-aws-and-other-market-leaders/.

[658] Li Nan 李楠, "直击 2018 云栖大会深圳峰会：阿里巴巴全面进军 IoT" [At the 2018 Yunqi Shenzhen Summit, Alibaba Makes a Full Commitment to IoT], *SooToo,* March 28, 2018, http://www.sootoo.com/content/675203.shtml.

[659] "Regions and Zones," Alibaba Cloud Services, accessed May 13, 2018, https://www.alibabacloud.com/help/doc-detail/40654.htm.

[660] "Alibaba Cloud International Website Privacy Policy," Alibaba Cloud Services, accessed May 13, 2018 https://www.alibabacloud.com/help/faq-detail/42425.htm.

and cloud storage will present U.S. IoT companies with increasingly serious questions about data supply chain integrity.

Corporate-Level Data Access

Although the explicit details of corporate-level data transfer are often difficult to obtain in the public domain, there are several likely means of corporate-level data access. Existing data privacy policies for major U.S. IoT companies frequently state that user data obtained through device and manufacturing level collection can be transferred in whole or in part to other companies, including through mergers and acquisitions or through separate data sharing, licensing, or purchase agreements. Although direct evidence of such data sharing between U.S. and Chinese firms is difficult to find, Chinese IoT firms writ large appear well-positioned to take advantage of this corporate willingness to share or sell user information.

Mergers and Acquisitions: Data as an Asset

One major type of authorized corporate-level data access is through corporate mergers and acquisitions. Chinese companies could access U.S. IoT data by simply buying U.S. IoT companies and their data. Several major U.S. IoT companies note that user data collected through use of a product may be transferred to the buyer or another entity upon the sale or transfer of the company or its assets.[661] Others acknowledge the possibility of data transfer in a merger, acquisition, or asset sale, but promise to notify the user.[662] The details of data transfer are typically hammered out in the process of corporate mergers and acquisitions, and are rarely mentioned in news reports and public announcements.

A prominent example of this type of corporate-level data access came to light during a mid-2016 attempt by Chinese technology company LeEco (乐视控股集团) to buy U.S. smart TV manufacturer Vizio. Vizio-brand smart TVs are equipped with "Automated Content Recognition (ACR)" technology, which collects detailed viewing information including identity of broadcast, TV provider, commercials and content viewed, device types, and associated network information like IP addresses if the user agrees.[663] This information is then paired with other demographic information like "sex, age, income, marital status, household size, education, home ownership, and household value" by a Vizio data subsidiary known as Inscape.[664] Vizio's data privacy policy acknowledges that information collected from users may be transferred to another company "…if the ownership of Vizio, Incorporated…changes as a result of a merger, acquisition [or] sale of assets,"[665] meaning that Chinese electronics firm LeEco likely would have received Vizio's

[661] Amazon, Nest, Vizio, and Belkin are among the companies that make such disclosures about possible transfer of collected data as part of corporate business transactions. For details, see the respective privacy policies of these companies, at "Amazon Privacy Notice," Amazon.com., updated August 29, 2017, accessed May 3, 2018, https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010; "Privacy Statement for Nest Products and Services," Nest Labs, effective November 1, 2017, accessed May 3, 2018, https://nest.com/legal/privacy-statement-for-nest-products-and-services/; "Privacy Policy," Vizio, Inc., effective October 26, 2017, accessed May 3, 2018, https://www.vizio.com/privacy; "Belkin Privacy Policy," Belkin International Inc., accessed May 3, 2018, http://www.belkin.com/us/privacypolicy/.

[662] "Welcome to the Google Privacy Policy," Google LLC.

[663] "Privacy Policy," Vizio, Inc., effective October 26, 2017, accessed May 3, 2018, https://www.vizio.com/privacy.

[664] Jacob Kastrenakes, "Most Smart TVs are Tracking You–Vizio Just Got Caught," *The Verge,* February 7, 2017, https://www.theverge.com/2017/2/7/14527360/vizio-smart-tv-tracking-settlement-disable-settings.

[665] "Privacy Policy," Vizio, Inc., effective October 26, 2017, accessed May 3, 2018, https://www.vizio.com/privacy.

collected user data as part of the agreement. LeEco's acquisition of Vizio ultimately fell through.[666] But if it had succeeded LeEco reportedly could have licensed Inscape data collection technology for use in its own televisions and could have kept all of Vizio's U.S. distribution agreements, [667] allowing LeEco to directly collect and analyze data from U.S. consumers.

While Vizio's sale to LeEco ultimately failed, other corporate acquisitions that could enable access to U.S. IoT data through authorized means are continuing apace. In March 2018, Foxconn, a Taiwanese technology company with close ties to China, announced that it would acquire U.S. firm Belkin, which includes networking equipment brand Linksys and makes Wemo brand home automation products.[668] Belkin's U.S. privacy policy states that information collected by Belkin through product use would be "transferred as a whole to the successor entity" in the event of a merger or acquisition.[669]

Data Brokers: Data as a Product

Corporate entities need not buy entire companies to access data, however. Instead, companies frequently buy or license data from third party data brokers that assemble information about consumers for monetary gain. While only limited evidence suggests that Chinese entities have specifically obtained U.S. IoT data, the increasing availability of this user information through data brokers could represent a major conduit for Chinese firms to eventually obtain U.S. IoT data at a large scale.

Some IoT companies have already sought to monetize the user data in their possession in response to the increased corporate appetite for aggregated user information. For instance, Vizio's data subsidiary Inscape bills itself as "the largest single source of opt-in smart TV viewing data available to license,"[670] and advertises data collection technology for television original equipment manufacturers.[671] LeEco had originally planned to license this data collection technology had it successfully acquired Vizio in 2016.[672]

Chinese companies, while not alone in their desire to obtain large quantities of data, are especially aggressive in collecting and using ever larger volumes of user information from IoT and smart devices.[673] Chinese data brokers are increasingly cooperating with U.S. companies to increase their access to data: China's largest data broker, TalkingData (北京腾云天下科技有限公司), boasts partnerships with Google, Baidu, Tencent, among many others.[674] The company claims to

[666] Sophia Yan, "Chinese Tech Firm LeEco's $2 Billion Acquisition of Vizio Stalled," *CNBC*, March 30, 2017, https://www.cnbc.com/2017/03/30/chinese-tech-firm-leecos-2-billion-acquisition-of-vizio-stalled.html.

[667] Bryan Bishop, "Vizio Acquired by Chinese Tech Company LeEco for $2 Billion," *The Verge,* July 26, 2016, https://www.theverge.com/2016/7/26/12286756/leeco-buys-vizio-tv-company-2-billion-acquisition.

[668] David Meyer, "Foxconn to Buy Consumer Electronics Company Belkin in Another Foreign Bid for a U.S. Firm," *Fortune*, March 27, 2018, http://fortune.com/2018/03/27/foxconn-belkin-china-iphone-linksys/.

[669] "Belkin Privacy Policy," Belkin International Inc., accessed May 3, 2018, http://www.belkin.com/us/privacypolicy/.

[670] "About," Inscape Data Services, accessed May 3, 2018, https://www.inscape.tv/about.

[671] "Solutions," Inscape Data Services, accessed May 3, 2018, https://www.inscape.tv/solutions#.

[672] Bishop, "Vizio Acquired by Chinese Tech Company LeEco for $2 Billion."

[673] While Chinese collection of genetic data through the creation of data centers like the China National Genebank and acquisition of 23andMe pose many of the same issues as the ones mentioned here, that sort of data collection is not being carried out in the context of IoT and is not included in this discussion.

[674] "合作伙伴" [Partners], TalkingData [北京腾云天下科技有限公司], accessed May 3, 2018, https://www.talkingdata.com/partners.jsp?languagetype=zh_cn.

collect data from more than 600 million smart devices on a monthly basis,[675] and announced in March 2016 that it had signed a partnership with U.S. firm Kochava to gain better tracking and ad measurement services for U.S. mobile applications.[676] In November 2017, TalkingData announced that it had would use Alluxio data acceleration systems to help unify its proprietary data sets generated by more than 120,000 mobile applications and 100,000 application developers.[677]

While direct evidence of expansive Chinese access to U.S. IoT data through data brokers is limited, data access through these means deserve further scrutiny. The market for data brokers is steadily expanding and data brokers are especially prolific in China, where one newspaper exposé revealed that private Chinese data brokers routinely amalgamated data on private citizens and sold revealing dossiers to customers for as little as $100.[678] The explosion in data made possible by IoT devices and the increasing Chinese appetite for data strongly suggests that U.S. IoT information will be an increasingly attractive commodity for acquisition by Chinese companies.

Other types of authorized data transfer may also be occurring at the corporate level, even if detailed information about the type and degree of data access is unavailable. Joint ventures between U.S. IoT companies and Chinese partners could lead to data sharing, especially in experimental contexts. Qualcomm's 2017 cooperative effort with Chinese IoT company Thundersoft (中科创达软件股份有限公司) to build a "Smart Car Cooperative Innovation Laboratory" (智能网联汽车协同创新实验室) will focus primarily on research and innovation of smart operating systems, user interfaces, and safety for smart cars[679]—tasks that could obviously benefit from data sharing between Qualcomm and Thundersoft. Though no specifics of any data sharing between Qualcomm and its Chinese counterpart could be found, Qualcomm collects potentially relevant statistics through its software and applications that can include device configuration information, device performance, and sensor data like motion, orientation, and environmental conditions.[680] Qualcomm's privacy policy notes that the company can share collected data as part of a "…merger, transfer, or other reorganization of all or parts of our business."[681] Ultimately, even if no U.S. IoT

[675] "About Us," TalkingData, Inc., accessed May 3, 2018, https://www.talkingdata.com/about-us.jsp?languagetype=en_us.

[676] Matt Marshall, "Mobile Analytics Company Kochava Strikes Deal to Give 80K Chinese Apps Access to U.S. Ads," *VentureBeat*, March 17, 2016, https://venturebeat.com/2016/03/17/mobile-analytics-company-kochava-strikes-deal-to-give-80k-chinese-apps-access-to-u-s-ads/.

[677] "China's Largest Data Broker Leverages Alluxio to Manage Terabytes of Data Across Disparate Data Sources," Alluxio, November 30, 2017, https://globenewswire.com/news-release/2017/11/30/1211869/0/en/China-s-Largest-Data-Broker-Leverages-Alluxio-to-Manage-Terabytes-of-Data-Across-Disparate-Data-Sources.html.

[678] Rao Lidong 饶丽冬 and Li Lin 李玲, "恐怖！南都记者 700 元就买到同事行踪，包括乘机、开房、上网吧等 11 项记录" [Terrifying! Southern Metropolis Reporters Use 700 RMB to Purchase Tracking of Colleagues, Including Motorcycle Movements, Housing, Internet Café Activities and 11 More Records], *南方都市报 Southern Metropolis*, December 12, 2016, http://epaper.oeeee.com/epaper/A/html/2016-12/12/content_103959.htm?from=timeline&isappinstalled=0&winzoom=1.

[679] "中科创达携手高通在渝打造智能创新平台 赋能智能汽车、物联网产业创新" [Thundersoft Links Arms with Qualcomm to Build Smart Innovation Platform in Chongqing for Innovation in Smart Cars, Internet of Things Products], 中科创达软件股份有限公司 Thundersoft, October 10, 2017, https://www.thundersoft.com/index.php/News/show/4-5-11-310.

[680] "Qualcomm Software and Applications," Qualcomm, Inc., accessed May 3, 2018, https://www.qualcomm.com/site/privacy/services.

[681] "Privacy Policy," Qualcomm, Inc., accessed May 3, 2018, https://www.qualcomm.com/site/privacy.

data is currently being shared with Thundersoft through Qualcomm, Qualcomm appears to reserve the right to do so in the future.

Some potential means of corporate-level data access, however, might carry substantially less risk for authorized corporate-level data transfer of U.S. user information. China's recent data localization laws have compelled several high-profile U.S. technology companies to store Chinese user data within China, attracting significant criticism from U.S. companies and the U.S. government.[682] However, while the domestic storage of Chinese data held by U.S. IoT companies operating in China enhances China's censorship and mass surveillance efforts and hardens its resiliency against foreign influence on the Internet,[683] it also poses a substantially less severe authorized data transfer risk to U.S. IoT data at the corporate level, as long as U.S. technology companies ensure that only Chinese user information is stored in China, and U.S. user data is stored outside of China.

Overall, the relative absence of details about corporate-level data transfer speaks to the lack of transparency in corporate-level data access. The receptiveness of U.S. IoT companies to data sharing, the broad scope of user information collected in aggregate, and aggressive efforts by Chinese companies to obtain data, however, indicate that corporate-level data sharing between U.S. IoT firms and Chinese counterparts is a potentially important conduit for data access.

Government Data Appropriation

The most sweeping potential means of data access are present at the nation-state level, where Chinese state planning papers and legal statutes lay out the rationale and justification for broad data access by China's government. These official documents are the clearest articulations of China's drive to obtain large amounts of data, an effort that virtually assures that any data in the hands of Chinese companies could potentially be appropriated by the Chinese government.

Several key state planning documents show China's economic planners view the data generated by the Internet of Things as a strategically vital catalyst for economic competitiveness. For example:

- In August 2015, the State Council issued an official government document known as a *gangyao* (纲要)[684] calling for the promotion of big data development in various industries supported by the Internet of Things and for China to become a "Strong Big Data Country

[682] United States Trade Representative, "2017 Report to Congress on China's WTO Compliance," January 2018, https://ustr.gov/sites/default/files/files/Press/Reports/China%202017%20WTO%20Report.pdf; William Mauldin, "U.S. Lawmakers Complain about China's Cloud Computing Restrictions," *Wall Street Journal,* March 23, 2017, https://blogs.wsj.com/washwire/2017/03/23/u-s-lawmakers-complain-about-chinas-cloud-computing-restrictions/.

[683] For an example of how foreign cloud storage services used to provide a way to bypass Chinese censorship, see Jeff South, "Punching a Hole in the Great Firewall," *ChinaFile*, March 21, 2014, http://www.chinafile.com/Punching-Hole-Great-Firewall. For an example of how Chinese data localization pressures work to close these bypasses, see Cate Cadell, "Amazon Sells Off China Cloud Assets as Tough New Rules Bite," Reuters, November 14, 2017, https://www.reuters.com/article/us-china-amazon-cloud/amazon-sells-off-china-cloud-assets-as-tough-new-rules-bite-idUSKBN1DE0CL.

[684] Roughly translated as "outline" in English, *gangyao* are typically characterized as authoritative policy directives issued by the highest organizations in the Chinese governing apparatus. The Chinese transliteration is left in the text to enhance contextual understanding of the concept, rather than using an approximate English translation of a uniquely Chinese concept.

(数据强国).”[685] The *gangyao* regards big data as a “transformative force for economic development, an important new opportunity for national competitiveness, and a new path for promoting better governance,” and specifically refers to big data, the Internet of Things, cloud computing, remote sensing, and mobile internet as critical enablers of future economic development.[686]

- MIIT’s 2017 “Plan for Big Data Industry Development (2016–2020),” (大数据产业发展规划(2016－2020 年)) describes data as a “national foundational strategic resource” (国家基础性战略资源) and the “diamond ore of the 21st century” (21 世纪的 “钻石矿”), highlighting the strategic value placed upon aggregated data.[687]

China’s highest officials regard data as a critical determinant of Chinese government’s overall national security and therefore subject to access, appropriation, control, and aggregation. In 2017, CCP Chairman Xi Jinping explicitly framed data security as a matter of maintaining national security and social stability in a speech about implementing China’s “National Big Data Strategy” (国家大数据战略).[688] This effort to leverage and control data is exemplified by an elaborate tapestry of Chinese laws mandating cooperation and access to information, including national security, cybersecurity, counter-terrorism, counter-espionage, and intelligence-gathering statutes.[689] Chinese government agencies are given wide berth through these legal provisions to demand cooperation from all Chinese companies and possibly foreign entities operating in China, as demonstrated below. (Translations of relevant legal statutes are included in Appendix B.) The ability of the Chinese government to access all data stored in China or collected by Chinese IoT companies is a distinguishing characteristic of the Chinese government’s approach to data writ large.

Justification for data appropriation by the Chinese government is frequently based upon China’s broad and distinct interpretation of its national security concerns. For instance, the 2015 National Security Law (国家安全法) outlines an expansive definition of China’s national security and pays special attention to various aspects of national security:

- Article 3 of the 2015 National Security Law places political, economic, military, cultural, and societal security under the purview of national security work.[690]
- Article 25 of the same law regards control of network and information technology as an integral component of national security, and requires the data of key internet and

[685] “Plan for Big Data Industry Development (2016–2020)” (大数据产业发展规划（2016－2020 年）), Ministry of Industry and Informatization Technology, January 17, 2017, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c5464999/content.html.

[686] “Outline for Promoting Big Data Development Actions” (促进大数据发展行动纲要), State Council of the People’s Republic of China, August 31, 2015, http://www.gov.cn/zhengce/content/2015-09/05/content_10137.htm.

[687] “Plan for Big Data Industry Development (2016–2020)” (大数据产业发展规划（2016－2020 年）), Ministry of Industry and Informatization Technology, January 17, 2017, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c5464999/content.html.

[688] Li Haiyun 李海韵, ed., “习近平：实施国家大数据战略加快建设数字中国” (Xi Jinping: Implement National Big Data Strategy and Accelerate Construction of Digital China), Xinhua Net 新华网, December 9, 2017, http://www.xinhuanet.com/2017-12/09/c_1122084706.htm.

[689] Approximate translations of relevant legal statutes are included in Appendix B.

[690] “中华人民共和国国家安全法” (National Security Law of the People’s Republic of China), National People’s Congress of the People’s Republic of China, accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm.

information systems to be "secure and controllable" (安全可控), suggesting that data is subject to inspection and review by government authorities for national security reasons.[691]

Chinese laws offer exceptionally broad definitions of the type and scope of potential data appropriation, often mandating cooperation from people and organizations in China in lieu of detailed parameters for data to be handed over. For example:

- Article 28 of the Cybersecurity Law (国家网络安全法) notes that all "network operators (网络运营者) should provide technical support and aid to public and national security organizations engaged in protection of national security and surveillance of criminals," without specifying the type or scope of this technical support.[692]
- Article 14 of the Intelligence Law (国家情报法) specifies that state intelligence organizations can "request support, aid, and coordination from relevant organs, organizations, and citizens" in the course of intelligence work, suggesting another possible means of data transfer to government authorities.[693]
- Article 10 of the Counter-Espionage Law (反间谍法) allows national security personnel to enter previously restricted areas to consult or seize relevant files and information, and Article 12 allows national security organs to carry out technical reconnaissance against relevant parties as needed.[694]
- Under Article 18 of the Counter-Terrorism Law (反恐怖主义法), telecommunications and internet providers are required to provide access and interface information and available decryption keys in support of anti-terrorist surveillance activities.[695]

Each of these statutes leaves open the possibility of extensive and largely open-ended data appropriation by the Chinese government for a wide range of circumstances.

Jurisdiction over which entities must cooperate with Chinese authorities is similarly broadly defined. Moreover, these statutes appear to include all Chinese companies and citizens within the scope of the various laws that might enable data appropriation. For example:

[691] "National Security Law of the People's Republic of China," National People's Congress of the People's Republic of China.

[692] "中华人民共和国国家安全法" (National Cybersecurity Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

[693] "中华人民共和国国家情报法" (National Intelligence Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm.

[694] "中华人民共和国反间谍法" (National Counter-Espionage Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2014-11/02/content_1884660.htm.

[695] National People's Congress of the People's Republic of China, "中华人民共和国反恐怖主义法" (National Counter-Terrorism Law of the People's Republic of China), Xinhua, accessed May 10, 2018, http://www.xinhuanet.com/politics/2015-12/27/c_128571798.htm.

- Article 80 of the National Security Law calls for citizens and organizations to support the operations of national security work.[696]
- Article 76, Sections 3 and 4 of the Cybersecurity Law note that "network operators" include administrators and network service providers, and "network data" includes all information collected, stored, transmitted, produced, and handled on a network.[697]
- Article 3 of the Detailed Regulations on Counter-Espionage Law Implementation (中华人民共和国反间谍法实施细则) extends the potential scope of the Counter-Espionage Law abroad to include "foreign organs, organizations in China with subsidiaries, and persons living in China without Chinese citizenship."[698]

Data Appropriation in Practice

While the Chinese government regards the collection of data as both a matter of economic policy and a concomitant feature of Chinese national security law, the actual implementation of these legal and economic policies is an important determinant of the risks to U.S. IoT data. Publicly documented instances of legal Chinese government appropriation of U.S. data are rare, and there are essentially no publicly documented examples of Chinese government appropriation of U.S. IoT data.

What might explain the dearth of information regarding legal or policy-level IoT data appropriation? One obvious answer is that the implications of the massive amount of data from the IoT have not yet fully resonated with the general public given the relatively nascent adoption of the IoT. While businesspeople, data privacy advocates, and technical specialists are almost certainly aware of the implications of big data resulting from the IoT, most users may regard the small amounts of collected IoT data as mundane and trivial. Individual temperature preferences collected by a smart thermostat may seem inconsequential in isolation, therefore failing to attract the attention and imagination of users who might otherwise object to any government access to their IoT data.

Another possible explanation, however, is that public disclosure of Chinese government appropriation of U.S. IoT data might be met with outrage, providing a strong incentive for Beijing to execute any such data access quietly and without fanfare. In 2007, the U.S. House Foreign Affairs Committee publicly upbraided U.S. tech company Yahoo for handing over IP information and email records of Chinese dissidents to the Chinese government.[699] It is unlikely that Chinese authorities would seek to attract further attention to any compulsory efforts to obtain data, and any future government attempts to access U.S. IoT data would likely be carried out quietly.

[696] "中华人民共和国国家安全法" (National Security Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm.

[697] "中华人民共和国国家安全法" (National Cybersecurity Law of the People's Republic of China), National People's Congress of the People's Republic of China, accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm.

[698] "中华人民共和国反间谍法实施细则" (Detailed Regulations on Counter-Espionage Law Implementation), State Council of the People's Republic of China, accessed May 10, 2018, http://www.gov.cn/zhengce/content/2017-12/06/content_5244819.htm.

[699] Jacqui Cheng, "Congress Unimpressed by Yahoo Apology for China Dissident E-Mail Testimony," *Ars Technica*, November 6, 2007, https://arstechnica.com/tech-policy/2007/11/yahoo-calls-withholding-of-info-on-chinese-arrests-a-misunderstanding/.

Although reliably documented instances of Chinese government appropriation of U.S. IoT data are practically nonexistent, legal and policy-enabled access to U.S. IoT data constitutes a unique risk to U.S. data privacy. While the main conduits of authorized data access at the user-level, the device level, and the corporate level are applicable to nearly all countries deploying the IoT, China's legal and policy measures for data appropriation present a distinctive challenge for U.S. data privacy. The implications of China's unique, high-level approach to data access are described in further detail below.

Impact on the United States

Authorized or non-forbidden access to IoT data is especially important for a variety of reasons. Data collected by the IoT represents both a qualitative and quantitative explosion in the amount of information made available through electronic means, expanding data collection beyond our online and virtual lives to potentially every aspect of our physical lives. Obtaining this information through permissive means is a comparatively low-cost way of acquiring extremely detailed information about IoT users, as demonstrated above.

Successful data acquisition is especially important for China's economic interests, particularly because of Beijing's emphasis on the development of AI and machine learning. Effective AI and machine learning efforts depend upon the availability of large quantities of data for training and improvement. China already has a sizable advantage in data collection because of its large population and lax privacy restrictions. Any additional data collection from outside of China would be greatly beneficial to China's efforts to become an international leader in AI technology. Chinese economic planners have explicitly linked big data and IoT development to China's artificial intelligence development efforts. For instance, the State Council's 2017 "New Generation Artificial Intelligence Development Plan (新一代人工智能发展规划)" prioritizes the development of IoT components like smart sensors and integrated circuits, and clearly acknowledges the critical role of large amounts of data to China's AI development efforts.[700]

The central concern surrounding Chinese access to U.S. IoT data is government data appropriation. This is unsurprising given the government's high prioritization of big data and the means to acquire it through the IoT. While the other conduits for access to U.S. IoT data are substantial and can vacuum up large quantities of U.S. IoT information, available evidence suggests that Chinese use of user-level, device-level, and corporate-level data access methods are not necessarily quantitatively or qualitatively different than the methods used by other countries, companies, or third-party entities. However, Beijing's sweeping government mandates make data appropriation by the Chinese government a substantial threat to U.S. IoT data privacy.

In the short term, Chinese access to U.S. IoT data could also jeopardize U.S. national security interests, providing ample means to establish pattern-of-life surveillance efforts for intelligence targets and improving artificial intelligence used for military applications. Chinese scholars writing in a publication sponsored by Chinese defense R&D organizations describe an increasing fusion between the information space, physical space, and human activities enabled by the IoT, and have cited scholarship describing the importance of big data in mapping out people's ever-

[700] "新一代人工智能发展规划" (New Generation Artificial Intelligence Development Plan), State Council of the People's Republic of China, July 8, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

changing patterns of life.[701] Chinese military commanders have already recognized the importance of big data, cloud computing, and the IoT to accelerate military decision-making processes.[702] In the long term, China's collection of U.S. IoT information would almost certainly be fed into state-led efforts to develop AI and machine learning, which could eventually translate into economic superiority in a burgeoning sector of future economic competition, as well as military superiority as the Chinese military begins to apply artificial intelligence capabilities for battlefield use.

It is important to note that while many of the major conduits for authorized data access described above are common characteristics of IoT development in all countries, China's state-level motivations and authorizations for accessing IoT data pose a unique challenge to U.S. economic and national security. All of the data acquisition methods described in this chapter are authorized, or at least non-forbidden, meaning that they and the information they collect are legal not expressly forbidden. What protections, if any, exist to secure U.S. IoT data?

Existing Protections for U.S. Data

The United States has no single, comprehensive federal law governing the collection and use of personal data. Instead, the existing U.S. data protection regime is composed of a patchwork collection of federal and state laws, principles, rules, regulations, and guidelines that address various aspects of data protection. These provisions occasionally overlap, complement, and contradict one another with different degrees of enforcement. For instance, guidelines developed by government agencies and industry groups do not have the force of law, but are instead considered "best practices" that are increasingly used as a basis for enforcement.[703]

Several federal laws regulate different aspects of data privacy and sensitive personal information in the United States, including consumer protection, financial and medical information, consumer credit, email addresses and phone numbers, and interception of electronic communications and computer tampering. Several of the most prominent and commonly applied laws are summarized in the table below.

[701] Yang Xiaogang 杨晓刚, Jiang Yi 姜毅, Zhang Ta 张塔, and Wang Weijun 王伟军, "基于大数据技术的用户小数据管理" (Small Data Management of Users Based on Large Data Technology), *情报理论与实践 Information Studies: Theory and Application* 41, No. 3, (2018): 29-30. *Information Studies: Theory and Application* is managed by state-run weapons manufacturer China North Industries Group Corporation (中国兵器工业集团有限公司; NORINCO Group) and published by the China Society for Defense Scientific and Technical Information (中国国防科学技术信息学会) and the NORINCO 210 Research Institute (中国兵器工业集团 210 研究所). Also known as the China Ordnance Industry Information Institute (北方科技信息研究所), the latter is a research and development organization focusing on applied information technology, big data, and intelligence. See "源—关于信息与情报的思考" [Intelligence, An Ever Scarcer Strategic Resource–Thoughts Regarding Information and Intelligence], 北方科技信息研究所 China Ordnance Industry Information Institute, June 25, 2013, http://www.norincogroup.com.cn/art/2013/6/25/art_158_32657.html.

[702] Li Qiaoming 李桥铭, "大数据：让战争指挥决策更科学" (Big Data: Making Warfare Command Decision-making More Scientific), China Military Online, March 3, 2017, http://www.81.cn/wj/2017-03/03/content_7512381.htm.

[703] Ieuan Jolly, "Data Protection in the United States: Overview," *Thomson Reuters Practical Law*, July 1, 2017, https://uk.practicallaw.thomsonreuters.com/6-502-0467.

Table 9: Summary of Federal Data Privacy Laws[704]

Federal Law	Role in Data Protection
Federal Trade Commission Act (FTCA)	Prohibits unfair or deceptive practices against consumers and has been applied to online privacy and data security
Financial Services Modernization Act (Gramm-Leach-Bliley Act; GLBA)	Safeguards consumer financial data
Health Insurance Portability and Accountability Act (HIPAA)	Protects sensitive health care information
Fair Credit Reporting Act (FCRA)	Protects accuracy, fairness, and privacy of consumer credit information in the files of consumer reporting agencies
Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)	Regulates the collection and use of e-mail addresses
Children's Online Privacy Protection Rule (COPPA)	Regulates the collection of information from and about children under the age of 13
Telephone Consumer Protection Act	Regulates the collection and use of telephone numbers
Electronic Communications Privacy Act	Regulates interception of electronic communications
Computer Fraud and Abuse Act	Regulates computer tampering

Certain states have also enacted laws to provide additional protection of U.S. data, mostly designed to address, deter, and punish unauthorized access and security breaches. California, for instance, is especially prolific in enacting data privacy laws. It was the first state to adopt a security breach notification law, setting a precedent that other states and territories have followed. California also has a law prohibiting smart televisions with voice recognition capabilities from using recorded words and conversations for advertising, making it one of the few states specifically addressing data privacy in the age of the IoT.[705] As of March 2018, all 50 states and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted legislation requiring people and businesses with licensed access to data to notify affected consumers of security breaches involving personal

[704] The information in this table is derived from several sources, including Jolly, "Data Protection in the United States: Overview"; "Gramm-Leach-Bliley Act," United States Federal Trade Commission, accessed May 11, 2018, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act; "Your Rights Under HIPAA," United States Department of Health and Human Services, accessed May 11, 2018, https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html; "A Summary of Your Rights Under the Fair Credit Reporting Act," United States Federal Trade Commission, accessed May 12, 2018, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf; "Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)," United States Federal Trade Commission, accessed May 12, 2018, https://www.ftc.gov/enforcement/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act; "Children's Online Privacy Protection Rule ("COPPA")," United States Federal Trade Commission, accessed July 5, 2018, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

[705] "Privacy Laws," State of California Department of Justice, Office of the Attorney General, accessed May 12, 2018, https://oag.ca.gov/privacy/privacy-laws/.

information.[706] Efforts to adapt state data privacy laws to the challenges of emerging technologies are ongoing.

Other efforts like industry and regulatory guidelines serve to regulate data privacy but stop short of binding legal force. Various industry and regulatory groups have outlined best practices for data protection that are used for self-regulation. For instance, the Digital Advertising Alliance's Self-Regulatory Principles lays out privacy practices for "multi-site data and cross-app data gathered in either desktop or mobile environments."[707] National regulatory bodies have also issued best practices. In 2015, the U.S. Federal Trade Commission (FTC) released a report containing "best practices" and other findings regarding privacy and security issues of the IoT.[708] The FTC is also responsible for enforcing voluntary supranational data protection codes of conduct, namely the APEC Cross-Border Privacy Rules (CBPR) System, which helps regulate cross-border flows of personal information.[709] Many of these guidelines are voluntary and not legally enforceable; notably, China is not a party to the APEC CBPR system.[710]

Many of those data privacy provisions that are legally enforceable typically fall under the authority of the FTC and are enforced under the provisions of the FTCA. The FTC's enforcement actions are predicated upon the agency's consumer protection mandate to punish "unfair or deceptive acts or practices in or affecting commerce."[711] This statute does not regulate specific categories of data but instead prohibits unfair and deceptive practices that fail to protect personal information. The FTCA's authority applies to most companies and individuals doing business in the United States.[712] Recent FTC data-related enforcement actions have included investigations into lax data protection practices at ride-sharing company Uber and surreptitious data collection practices at Vizio.[713]

The U.S. government appears increasingly aware of data privacy issues posed by the proliferation of the IoT. The recently introduced Internet of Things Cybersecurity Improvement Act of 2017 would mandate that suppliers of IoT devices to the U.S. government abide by a variety of security standards and procedures.[714] For its part, the FTC has implemented several initiatives to bolster the data privacy of IoT devices in the consumer world, including distributing primers for

[706] Jolly, "Data Protection in the United States: Overview."

[707] "DAA Self-Regulatory Principles," Digital Advertising Alliance, accessed May 12, 2018, http://digitaladvertisingalliance.org/principles.

[708] "Internet of Things: FTC Staff Report," United States Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[709] "Cross Border Privacy Rules System," APEC Electronic Commerce Steering Group, accessed May 12, 2018, http://www.cbprs.org/.

[710] "Cross Border Privacy Rules System," APEC Electronic Commerce Steering Group, accessed May 12, 2018, http://www.cbprs.org/.

[711] See § 45 of the Federal Trade Commission Act. "Federal Trade Commission Act," United States Federal Trade Commission, accessed May 12, 2018, https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf.

[712] Ieuan Jolly, "Data Protection in the United States: Overview."

[713] "Privacy and Data Security Update: 2017," United States Federal Trade Commission, January 2017-December 2017, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf.

[714] Anna Rudawski, "U.S. Senators Introduce IoT Cybersecurity Bill," *Data Protection Report,* August 3, 2017, https://www.dataprotectionreport.com/2017/08/senators-introduce-iot-cybersecurity-bill/.

businesses[715] and sponsoring competitions to solicit technical security tools that could improve IoT privacy.[716]

U.S. Data Protections: An Inadequate Approach

Despite recent enforcement actions and a new awareness of the issues at hand, current U.S. efforts at data protection are mixed. While some enforcement actions may be somewhat effective in protecting consumers, by and large, the existing protections and ongoing efforts to secure U.S. data outlined above are not up to the task of protecting U.S. data against authorized or non-forbidden data access, especially government-level data acquisition by foreign powers. Generally speaking, existing regulations for authorized data access do not account for the types of data collected by IoT devices and do not consider the broader economic and national security implications of Chinese access to U.S. data.

Many of the statutes identified above regulate specific categories of sensitive personal information, but none of them specifically account for the extremely detailed data collection that is a hallmark of IoT devices. At the user-level, IoT devices collect data that can facilitate deeply detailed analysis of a user's physical preferences, habits, status, and well-being. FTC staffers and experts recognize the privacy challenges that IoT devices present, noting that the sheer volume and detail of data collected by IoT devices may allow an entity to infer sensitive information without actually collecting it from a consumer.[717] At the time of writing, however, there does not appear to be any federal legal regulation governing the types of data collected by IoT devices or what can be done with collected data when aggregated. The FTC Act statue empowering the Commission to prosecute "unfair and deceptive" practices may not apply if a Chinese IoT company openly declares that it collects detailed user data and may transfer it to the Chinese government if asked. For example, Xiaomi's U.S. privacy policy retains the right to transfer personal information outside of the user's jurisdiction in accordance with applicable laws; further, it reserves the right to store data from the U.S. in its overseas data centers, including its site in Beijing.[718]

Existing regulations also do little to account for corporate-level data access that could pass U.S. IoT data to Chinese companies, where it could eventually wind up in the hands of the Chinese government. A 2013 report by the U.S. Government Accountability Office found that there was no unified federal law governing the "collection and sale of personal information among private-sector companies," with many of the existing regulations stemming from various federal laws with limited scope, like the Fair Credit Reporting Act.[719] The FTC also voiced its concerns in a May 2014 report calling for increased transparency from data brokers, noting that many brokers fell

[715] "Careful Connections: Building Security in the Internet of Things," United States Federal Trade Commission, accessed May 12, 2018, https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.

[716] "IoT Home Inspector Challenge," United States Federal Trade Commission, accessed May 12, 2018, https://www.ftc.gov/news-events/contests/iot-rules.

[717] "Internet of Things: FTC Staff Report," United States Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[718] "Privacy Policy," Xiaomi, Inc., updated May 6, 2016, http://www.mi.com/en/privacy/.

[719] "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," United States Government Accountability Office, September 2013, https://www.gao.gov/assets/660/658151.pdf.

outside the jurisdiction of the FCRA.[720] These concerns culminated in the introduction of the Data Broker Accountability and Transparency Act of 2015, which would have forced more transparency and collection restrictions upon data brokers.[721] The bill was referred to the Committee on Commerce, Science, and Transportation and has not passed as of May 2018. Even if the bill does eventually become law, it will likely do nothing to address foreign acquisition of U.S. data–the latest text of the bill contains no references to foreign entities that might buy data on U.S. consumers.[722]

Perhaps most concerning of all, the scattered nature of the current U.S. data protection regime makes it difficult to account for the broader economic and national security implications of Chinese access to U.S. data. Existing legal protections for U.S. data are primarily focused on personal privacy and consumer protection, and forthcoming legislation is frequently focused on addressing security vulnerabilities.[723] These approaches do not address the problems inherent to authorized data collection. For instance, the FTC is statutorily limited to investigating and prosecuting "unfair and deceptive" acts of data collection, which might stop unauthorized data collection but does little to stem data collection that is nominally approved by the user or not expressly forbidden. Even when national security concerns may stop data purchase or acquisition through mergers, such as the recent CFIUS rejection of the Ant Financial purchase of U.S. company MoneyGram,[724] national security authorities still may not have the legal tools to stop Chinese companies operating in the United States from handing over U.S. IoT data to the Chinese government.

Overall, existing U.S. data protections appear insufficient to the task of protecting U.S. data against harmful but authorized data access. In short, the patchwork nature of U.S. laws and authorities leaves loopholes that could facilitate Chinese access to U.S. IoT data in bulk, an especially risky proposition given known Chinese motivations for accessing big data. How, then, can these problems be mitigated?

Recommendations

The problems inherent in authorized Chinese access to U.S. IoT data and the weaknesses of existing U.S. data protections demand thoughtful proposals for reform. The following recommendations fall into two main categories.

Authorized Data Access in IoT:

Any attempt to address authorized Chinese access to U.S. data must begin by addressing authorized data access in IoT writ large. To that end, U.S. businesses and the federal government

[720] "Data Brokers: A Call for Transparency and Accountability," United States Federal Trade Commission, May 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[721] "S. 668–Data Broker Transparency and Accountability Act of 2015," United States Congress, accessed May 12, 2018, https://www.congress.gov/bill/114th-congress/senate-bill/668/text.

[722] Ibid.

[723] Anna Rudawski, "U.S. Senators Introduce IoT Cybersecurity Bill," *Data Protection Report,* August 3, 2017, https://www.dataprotectionreport.com/2017/08/senators-introduce-iot-cybersecurity-bill/.

[724] Greg Roumeliotis, "U.S. Blocks MoneyGram Sale to China's Ant Financial on National Security Concerns," Reuters, January 2, 2018, https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial/u-s-blocks-moneygram-sale-to-chinas-ant-financial-on-national-security-concerns-idUSKBN1ER1R7.

should implement the following recommendations based upon existing data privacy concepts like the Fair Information Practice Principles,[725] among others:

1. Enact a tiered disclosure regime broad enough to cover multiple aspects of authorized IoT data collection.

Categorizing IoT devices into "privacy tiers" could simplify disclosure of authorized data collection for distracted or disinterested users. Offering the ability to adjust privacy settings from "high privacy" to "medium" to "low" could convey detailed notification while preserving choice for the user.[726] Alternatively, grouping devices into privacy tiers could greatly simplify consumer choice while still providing detailed information about data collected. These privacy tiers could educate consumers about differentiated levels of risk resulting from different types of data collection: for instance, personal health data that might harm a patient might warrant additional warnings over device time of use data that might only be used for advertising purposes.

2. Mandate data expiration and de-identification of data according to existing principles of data minimization, especially for information resellers.

Any entity that uses collected IoT data should be required to disassociate collected information from specific user identities where possible and dispose of data after a set period. This shifts the burden of responsible use of data away from disinterested or distracted consumers and towards the users of the collected information, thereby mitigating the damage from potential security breaches or irresponsible or malicious use of aggregated information.[727] In cases where de-identification is not possible, data brokers and information resellers should be required to obtain specific collection and aggregation consent from consumers, disclose what data is available, and allow opportunities to correct inaccuracies or opt-out.

3. Codify these data regulations and others in a single, comprehensive federal law governing data privacy.

The existing patchwork collection of federal and state laws cannot hope to cover all types and aspects of authorized data collection, and industry guidelines and self-regulation have achieved little in the way of protection and transparency for consumers. A single, comprehensive federal law on data privacy would provide an accessible reference point for all types of data collection, including various types of IoT devices and the data they collect, as well as permissible and impermissible uses for the collected information. To avoid choking off data-driven innovation, statutes should be written in a technology-neutral way to account for new uses of data not accounted for at the original time of legislation.

[725] "Internet of Things: FTC Staff Report," United States Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[726] "Internet of Things: FTC Staff Report," United States Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[727] Internet of Things: FTC Staff Report," United States Federal Trade Commission, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Specific Risks Posed by Authorized Data Access by Chinese Actors:

While many of the methods of authorized data access apply to IoT products from all countries, the sweeping powers of the Chinese government to seize or obtain U.S. data collected by Chinese companies means that authorized data access by Chinese entities is a unique threat to U.S. economic and national security. Some possible remedies for this unique threat are described below.

1. Require foreign IoT products to disclose affiliation with foreign entities that may pose a significant risk of harmful but authorized access to U.S. data.

Disclosing the origin of IoT products would increase transparency and consumer awareness of the possible implications of authorized data access by foreign powers, while still preserving freedom of consumer choice in the marketplace. In the case of China, disclosure labels on IoT products should provide contextual information about the possible implications of authorized data access. A sample label could read:

> *"This product originates in whole or in part from a country which may compel its corporate entities to hand over any personal information collected by this device to the surveillance apparatus of that country without due process or in contravention of U.S. legal protections."*

2. Refer corporate-level attempts to transfer U.S. data to foreign entities to CFIUS for approval.

Attempts to transfer U.S. data to foreign corporate entities through mergers, acquisitions and asset sales, and information resale should be subject to CFIUS review, especially when the data concerned could accelerate Chinese military modernization efforts or enhance Chinese intelligence work. The January 2018 CFIUS review and subsequent rejection of Ant Financial's acquisition of MoneyGram indicates that there is already statutory precedent for this type of enforcement action.[728]

3. Expedite passage of a unified federal data privacy statute applicable to both foreign and domestic IoT companies.

The sooner a federal data privacy statute is enacted, the sooner foreign companies must comply with the same laws that U.S. companies do, thereby mitigating possible economic advantages that accrue to China through loopholes in U.S. data privacy protections. A degree of regulation at the federal level closes potential loopholes in authorized data access and leverages the specter of federal sanctions against foreign companies that fail to comply with U.S. law. The severity of federal sanctions can have enhanced deterrent value against foreign violators of U.S. law, as evidenced by recent sanctions enacted against ZTE for illicit commerce with Iran and North Korea.[729] Speed is critical: China's massive market and production capacity for IoT products means that its own standards and practices have a built-in importance and could displace fledgling U.S. regulations by sheer market share.

[728] Roumeliotis, "U.S. Blocks MoneyGram Sale to China's Ant Financial."

[729] Shannon Liao, "ZTE Is on Life Support After U.S. Ban," *The Verge*, May 9, 2018, https://www.theverge.com/2018/5/9/17336454/zte-us-phone-ban.

Conclusions and Areas for Further Research

China's unique approach to the development of IoT and its enabling infrastructure poses significant challenges for U.S. economic and national security interests. The highest echelons of the Chinese regime view IoT development and deployment as critical matters of China's economic competitiveness and national security. This perspective is widely held at the apex of the Chinese government and is barely concealed even when it causes controversy overseas. It permeates nearly all Chinese IoT policies, informing and justifying Beijing's drive to dominate international standards, extensive Chinese security research into exploitable IoT vulnerabilities, and the government's emphasis on acquiring data through the IoT. Taken together, China's state-centric approach to IoT development and the actions it undertakes to achieve its goals ultimately constitute a weighty challenge to U.S. economic and national security interests.

In some fields of IoT development, China's economic and national security-focused approach will call for substantial responses from U.S. policymakers. For instance, China's increasing participation in international standards committees will increasingly allow Beijing to dictate the rules of the road. The accelerating pace of Chinese research into IoT security vulnerabilities reflects Beijing's strong interest in IoT security is a function of national security and its abiding interest in exploiting these vulnerabilities in the nascent IoT. China's access to U.S. IoT data will only grow as Chinese IoT companies leverage their advantages in production and cost to gain market share in the United States. All of these fields of IoT development are part of Beijing's larger IoT policy and should not go unchallenged by U.S. industry and government.

Further research on the nature and scope of these challenges and some of the emerging countermeasures employed elsewhere such as the EU may help U.S. decision-makers craft more effective policy. A comprehensive accounting of Chinese participation in key international standards bodies would identify areas that might require more U.S. involvement. More exhaustive studies of the effectiveness of European data privacy protections may help determine what model of data protection would be most effective in closing the front door to the IoT data of U.S. citizens. Some of these countermeasures require only U.S. action and do not depend upon Chinese cooperation.

In other areas of IoT development, however, the U.S. ability to affect positive change will be limited. Asymmetries in IoT development caused by systemic differences between the U.S. and Chinese styles of government and economic structures are unlikely to be resolved by any single policy U.S. decision-makers could implement. For example, the one-party Chinese regime is simply more empowered to demand all data collected by Chinese IoT companies, including U.S. data. Although the U.S. government could theoretically prevent data held by U.S. companies from being turned over to Chinese entities, there is little it could do to prevent the Chinese government from obtaining such information once it is in the hands of Chinese companies. The Chinese government may exploit that information for strategic military or intelligence advantages, or hand it over to its favored "national champions" to enhance further IoT and AI development in ways that the U.S. government cannot do for U.S. companies in a free-market system.

In these cases, a clear-eyed understanding of the challenges and greater coordination and cooperation between industry and government will be needed more than ever. While industry and government are frequently at odds with each other, especially on questions of government regulation, the U.S. government and U.S. industry must come to a tacit understanding that the resources of Washington and the innovative capacity of the U.S. private sector must coordinate in order to counter the Chinese challenge in the IoT. Given the united front presented by Beijing, its standards committees, its civil-military IoT vulnerability research complex, and its legal regime for procuring data, there may soon be little other choice but for U.S. industry and government to coordinate.

The information and analysis contained in this report represent only an initial step in answering the challenge from China's IoT development policies. Further steps are needed: greater public and private-sector awareness, greater cooperation at home to remediate vulnerabilities without stymieing innovation, and a willingness to challenge China abroad in the standards committees that U.S. experts appear to have forsaken. The seriousness of the challenge from Chinese IoT policies will only increase in the years to come as the United States and China continue to engage in what amounts to a struggle for no less than the future of the Internet. The outcome of this struggle will ultimately rest upon the U.S. willingness to understand Chinese IoT development policies, and to develop sound policies of our own.

Appendix A: Comparison of Application Permissions for Home Management IoT Devices

	Google Home App[730]	Amazon Alexa App[731]	Xiaomi MiHome App[732]
Device and app history	N/A	• Can retrieve running apps	• Can retrieve running apps
Identity	• Can find accounts on the device • Can add or remove accounts	• Can find accounts on the device • Can add or remove accounts	• Can find accounts on the device • Can add or remove accounts
Contacts	• Can find accounts on the device	• Can find accounts on the device • Can modify the user's contacts	• Can find accounts on the device • Can read the user's contacts • Can modify the user's contacts
Calendar	N/A	N/A	• Can read calendar events plus confidential information • Can add or modify calendar events and send email to guests without the owner's knowledge
Location	• Can access precise location (GPS and network-based)	• Can access precise location (GPS and network-based)	• Can access approximate location (network-based) • Can access precise location (GPS and network-based)
SMS	• Can read user's text messages (SMS or MMS) • Can receive text messages (SMS)	• Can send SMS messages	• Can read user's text messages (SMS or MMS) • Can receive text messages (SMS)

[730] "Google Home," Google LLC, updated May 4, 2018, accessed May 11, 2018, https://play.google.com/store/apps/details?id=com.google.android.apps.chromecast.app&hl=en.

[731] "Amazon Alexa," Amazon Mobile LLC, updated May 10, 2018, accessed May 15, 2018, https://play.google.com/store/apps/details?id=com.amazon.dee.app&hl=en_AU.

[732] "Mi Home," Xiaomi Inc., updated April 24, 2018, accessed May 15, 2018, https://play.google.com/store/apps/details?id=com.xiaomi.smarthome&hl=en.

			- Can send SMS messages
Phone	N/A	- Can read phone status and identity	- Can directly call phone numbers - Can reroute outgoing calls - Can read call log - Can read phone status and identity - Can write call log
Photos/Media/Files	N/A	- Can read the contents of the user's USB storage - Can modify or delete the contents of the user's USB storage	- Can read the contents of the user's USB storage - Can modify or delete the contents of the user's USB storage
Storage	N/A	- Can read the contents of the user's USB storage - Can modify or delete the contents of the user's USB storage	- Can read the contents of the user's USB storage - Can modify or delete the contents of the user's USB storage
Camera	N/A	- Can take pictures and videos	- Can take pictures and videos
Microphone	N/A	- Can record audio	- Can record audio
Wi-Fi	- Can view Wi-Fi connections	- Can view Wi-Fi connections	- Can view Wi-Fi connections
Device ID and call information	N/A	- Can read phone status and identity	- Can read phone status and identity
Other	- Can receive data from Internet - Can view network connections	- Can power device on or off - Can interact across users	- Can download files without notification - Can interact across users

	• Can pair with Bluetooth devices • Can access Bluetooth settings • Can change network connectivity • Can connect and disconnect from Wi-Fi • Has full network access • Can run at startup • Can prevent device from sleeping • Can read Google service configuration	• Can receive data from Internet • Can view network connections • Can create accounts and set passwords • Can pair with Bluetooth devices • Can access Bluetooth settings • Can connect and disconnect from Wi-Fi • Can disable your screen lock • Can full network access • Can change your audio settings • Can run at startup • Can draw over other apps • Can use accounts on the device • Can control vibration • Can prevent device from sleeping	• Has full license to interact across users • Can transmit infrared • Can modify secure system settings • Can read Home settings and shortcuts • Can write Home settings and shortcuts • Has access to the Smartcard Service Permission label • Can view network connections • Can create accounts and set passwords • Can read battery statistics • Can pair with Bluetooth devices • Can access Bluetooth settings • Can send sticky broadcast • Can change network connectivity • Can allow Wi-Fi Multicast reception • Can connect and disconnect from Wi-Fi • Can disable your screen lock • Can control flashlight • Has full network access

			• Can change your audio settings • Can control Near Field Communication • Can read sync settings • Can run at startup • Can draw over other apps • Can use accounts on the device • Can control vibration • Can prevent device from sleeping • Can modify system settings • Can toggle sync on and off • Can install shortcuts • Can uninstall shortcuts

Appendix B: Selected Portions of Chinese Laws That Could Enable Data Access

Relevant Law	Article Number	Relevant Portion of Statute	Approximate English Translation
National Security Law[733]	3	国家安全工作应当坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全，构建国家安全体系，走中国特色国家安全道路。	National security work should support overall national security concepts, using the people's security as the aim, political security as the root, economic security as the foundation, and military, cultural, and societal security as the guarantees, relying upon international security as a support, protecting each field of national security, constructing a national security system, and walking the path of national security with Chinese characteristics.
	25	国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。	The state constructs a network and information support system, provides network and information security protection capabilities, strengthens network and information technology innovation, R&D applications, implements core network and information technology, and assures that information systems and data in key fields and foundational infrastructure are secure and controllable; it also strengthens network management, defense, prevention, and rule of law to punish network attacks, network intrusions, theft of secrets, spreading illegal information and other internet crimes in order to protect internet sovereignty, security, and development interests.

[733] National People's Congress of the People's Republic of China, "中华人民共和国国家安全法" (National Security Law of the People's Republic of China), accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm

	80	公民和组织支持、协助国家安全工作的行为受法律保护。	Citizens and organizations support and aid the operations of national security work.
Cybersecurity Law[734]	2	在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。	This law applies to construction, operation, protection, and use of internet inside the PRC, as well as internet security supervision and management.
	28	网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。	Network operators should provide technical support and aid to public security and national security organs protecting national security and surveilling criminal activities according to the law.
	37	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。	Personal information and important data generated or collected by operators of critical information infrastructure inside the PRC must store this information in China. Any information that is required to leave the country should rely upon security assessments according to laws from the MIIT and coordinated with the State Council.
	76	（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。 （四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。	3) Internet operators refer to all users on the network, all managers, and internet service providers. 4) Network data refers to all electronic data collected, stored, transmitted, handled, or produced through the internet.

[734] National People's Congress of the People's Republic of China, "中华人民共和国国家安全法" (National Cybersecurity Law of the People's Republic of China), accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

Intelligence Law[735]	11	国家情报工作机构应当依法搜集和处理境外机构、组织、个人实施或者指使、资助他人实施的，或者境内外机构、组织、个人相勾结实施的危害中华人民共和国国家安全和利益行为的相关情报，为防范、制止和惩治上述行为提供情报依据或者参考。	National intelligence work organs should hunt and handle intelligence on foreign organs, organizations, and individuals that jeopardize PRC national security or aid foreign organs, organizations, and individuals that do so.
	12	国家情报工作机构可以按照国家有关规定，与有关个人和组织建立合作关系，委托开展相关工作。	National intelligence work organs can construct cooperative relationships with relevant individuals and organizations according to relevant laws.
	14	国家情报工作机构依法开展情报工作，可以要求有关机关、组织和公民提供必要的支持、协助和配合。	National intelligence work organs can require relevant organs, organizations, and citizens to provide support, aid, and coordination according to the law.
Counter-Espionage Law[736]	10	国家安全机关的工作人员依法执行任务时，依照规定出示相应证件，可以进入有关场所、单	Personnel from national security organs may enter otherwise restricted relevant locations and units in the course of their duties after approval and showing proper

[735] National People's Congress of the People's Republic of China, "中华人民共和国国家情报法" (National Intelligence Law of the People's Republic of China), accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm

[736] National People's Congress of the People's Republic of China, "中华人民共和国反间谍法" (National Counter-Espionage Law of the People's Republic of China), accessed May 10, 2018, http://www.npc.gov.cn/npc/xinwen/2014-11/02/content_1884660.htm

		位；根据国家有关规定，经过批准，出示相应证件，可以进入限制进入的有关地区、场所、单位，查阅或者调取有关的档案、资料、物品。	credentials, and may read or seize relevant files, materials, and items.
	12	国家安全机关因侦察间谍行为的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施。	National security organs may carry out technical reconnaissance measures in conducting espionage work according to state regulations and after strictly approved procedures.
	20	公民和组织应当为反间谍工作提供便利或者其他协助。	Citizens and organizations should provide facilitating and other types of aid to counter-espionage work.
Detailed Regulations on Counter-Espionage Law Implementation[737]	3	《反间谍法》所称“境外机构、组织”包括境外机构、组织在中华人民共和国境内设立的分支（代表）机构和分支组织；所称“境外个人”包括居住在中华人民共和国境内不具有中华人民共和国国籍的人。	The “foreign organs and organizations” referred to in the Counter-Espionage Law specifically include foreign organs and organizations outside of China as well as their subordinate or representative components in China; “foreign persons” includes non-Chinese nationals living inside China.
Counter-Terrorism Law[738]	9	任何单位和个人都有协助、配合有关部门开展反恐怖主义工作的义务，发现恐怖活动嫌疑或者恐怖活动嫌疑人员的，应当及时向公安机关或者有关部门报告。	All units and individuals have the responsibility for aiding and coordinating with relevant departments to fulfill the duties of counter-terrorism work and must report terrorist or suspected terrorist activities and personnel to public security or relevant organizations.

[737] State Council of the People’s Republic of China, “中华人民共和国反间谍法实施细则” (Detailed Regulations on Counter-Espionage Law Implementation), accessed May 10, 2018, http://www.gov.cn/zhengce/content/2017-12/06/content_5244819.htm.

[738] National People’s Congress of the People’s Republic of China, “中华人民共和国反恐怖主义法” (National Counter-Terrorism Law of the People’s Republic of China).

	18	电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。	Telecommunications service operators and internet service providers must provide technical support and aid, including accesses and decryption keys, to investigating public security and national security organs.

Appendix C: Full Text of Selected IoT Company Privacy Policies

Huawei[739]

Huawei Consumer Business Privacy Statement

The Huawei Consumer Business Privacy Statement was updated on
April 15, 2018.

Huawei Device Co., Ltd. and its global affiliates (collectively, "Huawei", "we", "us", and "our") respect your privacy. Therefore, we have developed a Privacy Statement (hereinafter referred to as "this Statement") that covers how we collect, use, disclose, protect, store and transfer your personal data. Please take a moment to read and understand our privacy statement and let us know if you have any questions.

Personal data means any electronic or other information which alone or jointly with other information can be used to identify a natural person or make him/her identifiable. This Statement explains how Huawei processes your personal data, but does not cover all processing scenarios as you will be informed in specific processing activity. Therefore, before using a specific product or service, it is recommended that you read the privacy notice or supplementary statement released by Huawei for that product or service to understand how it processes your personal data.

This Statement applies only to Huawei personal and home products, including feature phones, smartphones, laptops, tablets, wearable devices, mobile broadband devices, smart household appliances, accessories, computer applications, mobile services, software, toolkits, websites, and services that display or mention this Statement.

This Statement describes:

1. How Huawei Collects and Uses Your Personal Data

2. How Huawei Uses Cookies and Similar Technologies

3. How Huawei Shares Your Personal Data

4. How Huawei Protects Your Personal Data

5. How You Can Manage Your Personal Data

6. How Huawei Protects Children's Personal Data

7. Links to Third-Party Websites, Products, and Services

[739] “Huawei Consumer Business Privacy Statement,” Huawei Technologies Co., accessed May 14, 2018 https://consumer.huawei.com/en/legal/privacy-policy/

I. How Huawei Collects and Uses Your Personal Data

A. Personal Data Collected by Huawei

Before using Huawei products or services, you may need to provide personal data. You do not have to provide your personal data to Huawei, but in some cases, the non-provision of certain personal data will cause the inability to provide you with some related products or services.

Huawei will collect and use your personal data for the purposes stated in this Statement. Here are some examples of personal data we may collect:

1. Personal data that you provide to Huawei

You need to register a Huawei ID to enjoy certain functions or services. When you register a Huawei ID or log in with a Huawei ID to shop online, download software, or purchase services, we will ask you to provide relevant personal data, such as your name, email address, mobile number, order information, shipping address, and payment mode.

Huawei may provide you with cloud storage services where you can sync and backup some of your files, pictures and data.

Some Huawei products allow you to communicate and share information with others. When you use a Huawei product to share things with your family and friends, you may need to create a Huawei ID that includes certain information which will be made public, including a nickname and avatar. Huawei may collect information related to those people, such as their names, email addresses, and phone numbers. Huawei will take appropriate and necessary measures to ensure the security of the information that you provide. You must ensure that the people, whose information you provide, have consented to you providing their information to Huawei.

To meet some jurisdictions' requirements on real-name authentication of accounts, prevention of electronic game addiction, or Internet payment, Huawei might ask you to provide a proof of identity issued by the government or relevant card information that can identify you.

2. Information that Huawei collects in your use of services

Huawei will collect data about your device and how you and your device exchange information with Huawei products and services. This type of information includes:

(1) Device and application information, such as the device name, device identification code (IMEI, ESN, MEID, and SN), device activation time, hardware model, OS version, application version, software identification code, and device and application settings (such as region, language, time zone, and font size).

(2) Mobile network information, such as the public land mobile network (PLMN) provider ID and Internet Protocol (IP) address.

(3) Log information. When you use Huawei services or view Huawei-provided content, Huawei will automatically collect and log some information, such as the time of access, access count, IP address, and information about incidents (such as errors, crashes, restarts, and upgrades).

(4) Location information. Huawei will collect, use, and process the approximate or precise location of your device when you access some location-based services (for example, when you search, use navigation software, or view the weather of a specific location). Location information can be obtained based on the GPS, WLAN, and service provider network ID. We will ask you to choose the applications for which you want to enable location services. In the device settings menu, you can disable the location permissions of specific services to reject sharing your location information.

(5) Information you store on Huawei servers. For example, the information you upload to the cloud will be stored on Huawei servers for rapid access and sharing between devices. We will not view the information you store on Huawei servers.

3. Information from third-party sources

When permitted by law, Huawei will collect information about you from public and commercial sources. Huawei may also obtain certain information from third-party social network services, such as the time when you use a social network account to log in to a Huawei website.

4. Collection and use of non-identifiable data

Non-identifiable data refers to data that cannot be used to identify an individual. Examples of non-identifiable data include statistics on website visits, application downloads, and product sales volume. Huawei will collect statistics information to understand how users use our products and services. By doing so, we can improve our services to better meet your requirements.

We keep your personal data and non-identifiable data separate, and use each independently. Circumstances may arise where Huawei collects, uses, discloses, and transfers non-identifiable data for other purposes at our own discretion.

B. How Huawei Uses Your Personal Data

Huawei may use your personal data for the following purposes:

(1) Register and activate Huawei personal and home products that you have purchased.

(2) Register a Huawei ID so that you can enjoy a wider range of functions and mobile services.

(3) Deliver, activate, or verify the products and services you have requested, or perform changes and provide technical support and after-sales services for the foregoing products and services based on your requirements.

(4) Send you OS or application updates and installation notifications.

(5) Provide personalised user experience and content.

(6) Send you information about products and services you might be interested in, invite you to Huawei promotional activities and market surveys, or send marketing information to you. If you do not want to receive such information, you can opt out at any time.

(7) Carry out internal auditing, data analysis, and research; analyse business operation efficiency and measure market shares; and improve Huawei's products and services.

(8) Synchronise, share, and store the data you have uploaded or downloaded, as well as the data needed for the upload and download operations.

(9) Improve our loss prevention and anti-fraud programmes.

(10) Process pursuant to laws and regulations, e.g. tax, authority requests.

(11) Other purposes within specific services or with your consent.

II. How Huawei Uses Cookies and Similar Technologies

A. Cookie

A cookie is a text file stored by a web server on a computer or mobile device, and the content of a cookie can be retrieved and read only by the server that created the cookie. Cookies are unique to the browser or mobile application you are using. The text in a cookie often consists of identifiers, site names, and some numbers and characters.

Sometimes, Huawei stores cookies on computers or mobile devices for the purpose of improving user experience, including the following scenarios:

(1) Technical cookies: Login and verification. When you use a Huawei ID to log in to a website, the “session-based” cookies ensure that your visit to this site functions as smoothly as possible. .

(2) Personalisation cookies: Storage of your preferences and settings. A website can use cookies to save settings, such as the language setting and font size on your computer or mobile device, items in your shopping cart, and other browser preferences.

(3) Advertising cookies. Huawei uses cookies to collect information about your online activities and interests and provide you with advertisements that correlate most highly with you.

(4) Statistical cookies. With cookies, Huawei can collect information about your use of our websites and other applications, either for a single visit (using a session cookie) or for repeated visits (using a persistent cookie).

(5) Social Media Cookies. Social media cookies are linked to services provided by third parties, such as ‘Like’ buttons and ‘Share’ buttons. The third party provides these services in return for recognising that you have visited our websites.

You can manage or delete cookies at your own preference. For details, visit AboutCookies.org. You can clear all the cookies stored on your computer, and most current web browsers provide the option of blocking cookies. However, blocking cookies will require you to change your user settings every time you visit our website. Find out how to manage cookie settings for your browser here: Internet Explorer > Google Chrome > Mozilla Firefox > Safari > Opera.

If you clear cookies, you will need to change your settings the next time you visit Huawei websites. Note that some Huawei services require the use of cookies. Disabling cookies may affect your use of some or all functions of these services.

B. Web Beacons and Pixel Tags

In addition to cookies, Huawei and some third parties may also use web beacons and pixel tags on websites. A web beacon is usually an electronic graphic image embedded into a website or email to identify your device cookies when you browse the website or email. Pixel tags allow Huawei to send emails in a way that is readable to you and find out whether an email is opened.

Huawei and some third parties use these technologies for various purposes, including analysing service usage (together with cookies) and providing more satisfactory content and advertisements to you. For example, when you receive an email from Huawei, it may contain a click-through URL which links to a Huawei web page. If you click the link, Huawei will track your visit to help us learn about your preferences for products and services and improve our customer service. You can unsubscribe from the mailing list of Huawei at any time if you do not want to be tracked in this manner.

C. Other Local Storage

Huawei and some third parties may use other local storage technologies, for example, local shared objects (also called "Flash cookies") and HTML5 local storage, in certain products and services. Similar to cookies, these technologies store information on your device and can record some information about your activities and preferences. However, these technologies may use different media from cookies. Therefore, you may not be able to control them using standard browser tools and settings. For details about how to disable or delete information contained in Flash cookies, click here.

D. Do Not Track

Many web browsers provide a Do Not Track function that can release Do Not Track requests to websites. Currently, major Internet standardisation organisations have not established policies to specify how websites should handle these requests. If you enable Do Not Track in your browser, all Huawei websites will respect your selection.

III. How Huawei Shares Your Personal Data

We do not share personal data with other companies, organisations and individuals unless one of the following circumstances applies:

(1) Sharing with consent: After obtaining your consent, Huawei will share the information that you have authorised with specified third parties or categories of third parties.

(2) Sharing pursuant to laws and regulations: Huawei may share your information as required by laws and regulations, for resolving legal disputes, or as required by administrative or judiciary authorities pursuant to law.

(3) Sharing with Huawei affiliates: Your information may be shared within Huawei's affiliates only for explicit, and legitimate purposes, and the sharing is limited only to information required by services. For example, we verify the global uniqueness of accounts before allowing them to be registered.

(4) Sharing with business partners: Some products and/or services are provided to you directly by our partners. Huawei also may share your information with them, they may use your information to provide you with products and/or services you request (e.g., products sold by third-party seller through Huawei’s e-commerce platform, video content provided by other companies through Huawei’s applications), make predictions about your interests and may provide you with advertisements, promotional materials and other materials

(5) Sharing with service providers: Huawei also may disclose your information to companies that provide services for or on behalf of us. Examples of these service providers include companies that provide hotline services, send email, or provide technical support on behalf of Huawei. The service providers can use your information only for the purpose of providing services to you on behalf of Huawei.

(6) Huawei will share your information when there is a reasonable requirement to do so, for example, to meet request of applicable law, regulation, legal process or enforceable government.

In scenarios 3 to 6, Huawei will ensure that the lawfulness of this sharing and sign stringent non-disclosure agreements (NDAs) and/or data processing clauses with the companies, organisations, and individuals with whom personal data is shared, requiring them to comply with this Statement and take appropriate confidentiality and security measures when processing personal data.

IV. How Huawei Protects Your Personal Data

Huawei attaches great importance to the security of your personal data and has adopted standard industry practices to protect your personal data and prevent it from unauthorised access, disclosure, use, modification, damage, or loss. To this end, Huawei takes the following measures:

(1) We take reasonable and feasible measures to ensure that the personal data collected is minimal and relevant to what is necessary in relation to the purposes for which they are processed. We retain your personal data for no longer than is necessary for the purposes stated in this Statement and privacy notice of specific product or service, unless extending the retention period is required or permitted by law.

(2) We use a range of technologies such as cryptographic technologies to ensure the confidentiality of data in transmission. We implement trusted protection mechanisms to protect data and data storage servers from attacks.

(3) We deploy access control mechanisms to ensure that only authorised personnel can access your personal data. In addition, we control the number of authorised personnel and implement hierarchical permission management on them based on service requirements and personnel levels.

(4) We strictly select business partners and service providers and incorporate personal data protection requirements into commercial contracts, audits, and appraisal activities.

(5) We hold security and privacy protection training courses, tests, and publicity activities to raise employees' personal data protection awareness.

Huawei is committed to protecting your personal data. Nevertheless, no security measure is perfect and no product, service, website, data transfer, computing system, or network connection is absolutely secure.

To cope with possible risks, such as personal data leakage, damage, and loss, Huawei has developed several mechanisms and control measures, clearly defined the rating standards of security incidents and vulnerabilities and corresponding processing procedures, and established a dedicated Security Advisory and Security Notice page. Huawei has established a dedicated emergency response team to implement security planning, loss reduction, analysis, locating, and remediation, and to perform tracking operations with related departments based on security incident handling regulations and requirements.

If any personal data incident occurs, Huawei will notify you, pursuant to relevant legal and regulatory requirements, of the basic information about the security incident and its possible impact, measures that Huawei has taken or will take, suggestions about active defense and risk mitigation, and remedial measures. The notification may take the form of an email, text message, push notification, etc. If it is difficult to notify data subjects one by one, we will take appropriate and effective measures to release a Security Notice. In addition, we will also report the handling status of personal data security incidents as required by supervisory authorities.

V. How You Can Manage Your Personal Data

A. Access, rectification, deletion, data portability, restriction of processing, objection to processing.

Legislation in some countries and regions to which Huawei provides products and services or from where Huawei processes personal data, provides that data subjects the rights request (hereinafter referred to as "requests") in regards to the accessing, rectifying, deleting or erasure, porting, restricting, and objecting, the processing of related personal data by Huawei retains. In addition you will have the right to data portability.

1. Requesting modes and channels

Data subjects' requests must be submitted in accordance with Huawei designated privacy channels. The requests are valid even when the requester does not specify the laws on which the requests are based.

Data subjects' requests may be initiated through the official website of Huawei Consumer BG, HiCare app or Huawei ID app. If a data subject initiates a request via a hotline, email, online customer service, service centre, or another channel, we will instruct the data subject to officially raise the request through one of the aforementioned channels to facilitate communication and feedback of progress and results. The dedicated request channels for data subjects are intended to protect data subjects' lawful interests, ensure Huawei's normal operation, and prevent the right to request from being misused or fraudulently used.

2. Validity of requests

Most laws require data subjects to comply with specific requirements when they initiate requests. This Statement requires data subjects to:

(1) Submit requests through dedicated request channels provided by Huawei (namely, the official website of Huawei Consumer BG, HiCare app, and Huawei ID app).

(2) Provide sufficient information for Huawei to verify their identities (to ensure those who initiate the requests are the data subjects themselves or those authorised by them).

(3) Ensure that their requests are specific and feasible.

There are some circumstances, provided by laws and regulations, in which Huawei may not have to comply with the request in full or at all.

B. Consent withdrawal

You can change the authorised personal data collection scope or withdraw your consent without affecting the lawfulness of the processing activities based on the consent and prior to such withdraw.

Your rights can be exercised by deleting information, disabling related functions, or setting privacy options on your Huawei product. Huawei will release the methods for withdrawing consent for specific products and services in the privacy notice or supplementary statement of those products and services or upon request according to section A above.

C. Deregistering a Huawei ID

You can deregister your account in Huawei ID-related products. After you deregister your account, we will stop providing products and services, and delete your personal data unless otherwise stipulated by law. Your account cannot be restored after deregistration. You need to register a new Huawei ID if you want to use related Huawei products or services again. You can submit a deregistration application and complete the process in setting menu after logging in to your Huawei ID on related devices, applications or official website.

VI. How Huawei Protects Children's Personal Data

Huawei's personal and home products are intended for adults. However, for the use of Huawei products and services by children, we are fully aware of the importance of taking extra preventive measures to protect privacy and security. Huawei identifies whether data subjects are children based on the age of majority defined by laws of the local countries and regions.

When children's personal data is collected based on the consent of the holders of parental responsibility, we will only use or disclose the information as permitted by law, explicitly consented to by the holders of parental responsibility, or required for protecting the children. Holders of parental responsibility who need to access, modify, or delete the personal data of their children and people under guardianship can contact us via the channels provided in "IV. How Huawei Protects Your Personal Data."

If Huawei accidentally collects children's personal data without obtaining consent from provable holders of parental responsibility, Huawei will delete the information as soon as possible after becoming aware of it.

VII. Links to Third-Party Websites, Products, and Services

Huawei websites, application software, products, and services may contain links to third-party websites, products, and services. Huawei products and services may also use or provide products or services from third parties, for example, third-party apps released on Huawei app store HiApp.

All links to third-party websites, products, and services are provided for users' convenience only. You need to determine your interaction with such links on your own. Before submitting your personal data to third parties, please read and refer to these third parties' privacy policies.

VIII. International Transfers of Your Personal Data

Our products and services are delivered through resources and servers located in different places, to offer our products and services, we may need to transfer your personal data among several countries. Authorised Huawei personnel and third parties acting on our behalf may access, use and process personal data collected from you in a country/region that is different from the country/region where you entered the personal data, which may have less stringent data protection laws. When we transfer your personal data to other countries/regions, we will protect that the personal data as described in this statement or as otherwise disclosed to you at the time the data is collected (e.g. via privacy notice or supplementary statement of specific product or service).

Huawei has implemented global privacy practices for processing personal data protected under various data protection laws. Huawei transfers personal data between the countries in which we operate in accordance with the standards and conditions of applicable data protection laws, including standards and conditions related to security and processing.

With respect to personal data coming from the EU or Switzerland, we comply with applicable legal requirements providing adequate safeguards for the transfer of personal data to countries outside of the European Economic Area ("EEA") or Switzerland. We use a variety of legal mechanisms, such as standard contractual clauses to implement the cross-border transfer of your personal data; or implement security measures like anonymisation on the data before the cross border data transfer.

IX. International Users

If you use Huawei consumer cloud services in a member state of the European Economic Area (EEA) or Switzerland, Albania, Andorra, Bosnia, Faroe Islands, Gibraltar, Greenland, Republic of Macedonia, Moldova, Monaco, Montenegro, San Marino, Serbia, Vatican, Japan, South Korea, the USA, and Canada, Aspiegel Limited in Ireland is the data controller.

If you use the US Huawei online store (www.hihonor.com/us), Huawei Device USA, Inc is the data controller.

If you use the Europe Huawei online store, Huawei Technologies Dusseldorf GmbH is the data controller.

X. Updates to This Statement

Huawei reserves the right to update this Statement at any time.

Should this Statement be revised from time to time, Huawei will release the change notice via various channels, for example, posting the latest version on our official website: http://consumer.huawei.com.

"Major changes" in this Statement include but are not limited to:

(1) Major changes in our service modes, for example, purposes of personal data processing, types of processed personal data, and ways of using personal data

(2) Major changes in our ownership structure, organisational structure, etc., for example, ownership changes caused by business adjustment, bankruptcy, or acquisition

(3) Changes in the main objects of personal data sharing, transfer, or disclosure

(4) Major changes in your rights regarding personal data processing and the ways in which you can enjoy those rights

(5) Changes of Huawei departments, contacts, and complaint channels responsible for the security of personal data processing

(6) High risks identified in personal data security impact assessment reports

XI. How to Contact Us

We have set up a dedicated personal data protection department (or data protection officer). If you have any questions, comments, or suggestions, please contact us by visiting the contact us page or submitting them to our global offices. To obtain the complete list of Huawei offices, please visit the global offices page.

Note: Due to differences in local laws and languages, the local versions of Huawei Consumer Business Privacy Statement may be different from this version. In the case of any conflicts, the local versions shall prevail.

Xiaomi[740]

Privacy Policy

Our Privacy Policy was updated on 25 April 2018 and will take effect on 25 May 2018. If you do not agree with these changes and no longer wish to use our service, you may cancel your account by emailing us at privacy@xiaomi.com.

We have revamped the Privacy Policy front and back so that from this date onwards, this Privacy Policy can provide privacy details on how we manage your personal information for all Xiaomi products and services, unless a separate privacy policy is provided for a specific Xiaomi product or service.

Please take a moment to familiarize yourself with our privacy practices and let us know if you have any questions.

Our commitment to you

This Privacy Policy sets out how Xiaomi Inc. and its affiliated companies within the Xiaomi Group (“Xiaomi”, “we”, “our” or “us”) collect, use, disclose, process and protect any

[740] “Privacy Policy,” Xiaomi Inc., accessed May 11, 2018, http://www.mi.com/us/about/new-privacy/

information that you give us when you use our products and services located at www.mi.com, en.miui.com, account.xiaomi.com, MIUI and our Suite of applications that we offer on our mobile devices, for a list of these applications, please click here. Should we ask you to provide certain information by which you can be identified when using Xiaomi products and services, it will only be used in accordance with this Privacy Policy and/or our terms and conditions for users.

The Privacy Policy is designed with you in mind, and it is important that you have a comprehensive understanding of our personal information collection and usage practices, as well as full confidence that ultimately, you have control of any personal information provided to Xiaomi.

In this Privacy Policy, “personal information” means information that can be used to directly or indirectly identify an individual, either from that information alone or from that information combined with other information Xiaomi has access about that individual. Such personal information may include but not limit to the information you provide to us or upload, the information specific to you that may be assigned by us, your financial information, social information, device or sim-related information, location information, log information.

By using Xiaomi products and services or other acting permitted by the applicable laws, you are deemed to have read, acknowledged and accepted all the provisions stated here in the Privacy Policy, including any changes we may make from time to time. In order to comply with applicable laws, including local data protection legislation (e. g. General Data Protection Regulation in Europe Union), we will specifically seek prior explicit consent to the particular processing (e. g. automated individual decision-making) of special categories of personal data. Furthermore, we are committed to protecting the privacy, confidentiality and security of your personal information by complying with applicable laws, and we are equally committed to ensuring that all our employees and agents uphold these obligations.

Ultimately, what we want is the best for all our users. Should you have any concerns with our data handling practice as summarized in this Privacy Policy, please contact privacy@xiaomi.com to address your specific concerns. We will be happy to address them directly.

If you have questions or concerns regarding our Privacy Policy or practices, please contact us at privacy@xiaomi.com. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request .

What information is collected and how can we use it?

Types of information collected

In order to provide our services to you, we will ask you to provide personal information that is necessary to provide those services to you. If you do not provide your personal information, we may not be able to provide you with our products or services.

We will only collect the information that is necessary for its specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We may collect the following types of information (which may or may not be personal information):

- **Information you provide to us or upload** (including your contact details): we may collect any and all personal information you provide to us, like your name, mobile phone number, email address, delivery address, ID card, driver license, passport details, Mi Account details (e.g. your security related information, name, birthday, gender), order, invoicing details, materials or data you may sync through Mi Cloud or other apps (e.g. photos, contact lists), information in relation to creating an account and participating in the MIUI Forum or other Xiaomi platforms, phone numbers you insert into your contacts or to send a message, feedback, and any other information you provide us.
- **Information specific to you that may be assigned by us:** we may collect and use information such as your Mi Account ID.
- **Information specific to you that may be assigned by Third Party Service Providers:** we may collect and use information such as your advertising ID assigned by Third Party Service Providers.
- **Financial information:** information related to completing purchases. For example, bank account number, account holder name, credit card number etc.
- **Social information:** information related to your social activities. For example, current employer, current job title, education background, professional training background etc.
- **Device or SIM-related information:** information related to your device. For example, IMEI number, IMSI number, MAC address, Serial number, MIUI version and type, Android version, Android ID, screen display information, device keypad information, device manufacturer details and model name, network operator, connection type, hardware usage information such as battery usage, device temperature.
- **Application information:** information related to your software usage. For example, application list, application status record (e.g. downloading, installing, updating, deleting), application ID information, SDK version, system update settings etc.
- **Location information** (only for specific services/functionalities): various types of information on your location. For example, region, country code, city code, mobile network code, mobile country code, cell identity, longitude and latitude information, time zone settings, language settings.
- **Log information:** information related to your use of certain functions, apps and websites. For example, cookies and other anonymous identifier technologies, IP addresses, network request information, temporary message history, standard system logs, crash information.
- **Other information:** environmental characteristics value (ECV) (i.e. value generated from Mi Account ID, phone device ID, connected Wi-Fi ID and location value).

We may also collect other types of information which are not directly or indirectly linked to an individual and which is aggregated, anonymized or de-identified. For example, the device model and system version number of the user’s Xiaomi mobile phone device may be collected when using a particular service. Such information is collected in order to improve the services we provide to you.

How the personal information can be used

Personal information is collected for providing services and / or products to you, and legal compliance on our part under applicable laws. You hereby consent that we may process and disclose personal information to our affiliated companies (which are in the communications, social media, technology and cloud businesses), Third Party Service Providers (defined below) for the purposes stated in this Privacy Policy.

We may use your personal information for the following purposes:

- Providing, processing, maintaining, improving and developing our goods and/or services to you, including after-sales and customer support and for services on your device or through our websites.
- Communicating with you about your device, service or any general queries, such as updates, customer inquiry support, information about our events, notices.
- Conducting marketing related activities, such as providing marketing and promotional materials and updates. For more information on marketing and promotional activities, please refer to the Direct Marketing section below.
- Allowing you to post comments in public forums.
- Conducting promotional activities, such as sweepstakes and Facebook events.
- Analyzing and developing statistical information on use of our products and services to better improve our products and services.
- Optimizing the performance of your device, such as analyzing the memory usage or CPU utilization of our applications.
- Storing and maintaining information about you for our business operations or legal obligations. Providing local services without communicating with our servers.

Here are more details on how we use your information (which may include personal information):

- **Setting up your Mi Account.** Personal information collected when creating a Mi Account on our web sites or through our mobile devices is used for creating the personal Mi Account and profile page for the user.
- **Processing your purchase orders.** Information relating to e-commerce orders may be used for processing the purchase order and related after-sales services, including customer support and re-delivery. In addition, the order number is used to cross check the order with the delivery partner as well as the actual delivery of the parcel. The receipt details, including name, address, phone number and postal code are for delivery purposes.

The email address is used to send parcel tracking information to the user. The list of purchased item(s) is used for printing the invoice and allowing users to see what is in the parcel.

- **Allowing you to participate in MIUI Forum.** Personal information in relation to the MIUI Forum or other Xiaomi Internet platforms may be used for profile page display, interaction with other users, participating in the forum.
- **Providing Mi Cloud and other MIUI services.** Information (device or SIM card-related information including IMEI number, IMSI number, phone number, device ID, device operating system, MAC Address, device type, system and performance information and location information including mobile country code, mobile network code, location area code and cell identity) is collected for activating MIUI services, e.g. Mi Cloud, call log sync, SMS sync, Find Device, for the purposes of user authentication and activation of the services.
- **Diagnosing activation failures:** Location related information is used for the purpose of assessing SIM card activation failure (i.e. failure of SMS gateway and network) to identify the network operator of that service, and notify the network operator of that failure.
- **Providing other MIUI services.** Other information collected for each of the MIUI services may be used for performing the functions of that service, and to facilitate the provision of that service for the benefit of the user, e.g. downloading, updating, registering or performing activities related to MIUI services. For example, personal information collected by the Theme Store may be used to provide personalized theme recommendation services based on your downloading and browsing history.
- **Finding your device:** Xiaomi's Find Device feature helps you find and secure your phone if it is lost or stolen. You can locate your phone on a map using location information provided by your phone, wipe your phone, or lock your phone. We may collect your location data directly from your mobile device, or in some situations, from cell towers or Wi-Fi hotspots.
- **Recording location information in photos.** You have the ability to record your location information while taking a photo. This information will be visible within your photos folder and the location will be put into the header of your photos. If you do not wish to have your location recording while taking a photo, you may turn this off at any time within the camera settings of the device.
- **Providing messaging functions (e.g. Mi Talk, Mi Message).** If you download and use Mi Talk, information collected for Mi Talk may be used for activating this service and identifying the user and message recipient. In addition, chat history is stored for the convenience of re-loading historical chats after a user has re-installed apps, or for synchronization across devices. Information (sender's and recipient's phone numbers and Mi Message IDs) may be used for Mi Message for activating the services and enabling the service to function, including routing of messages.
- **Providing location based services.** In the course of using MIUI services, location information may also be used by us or Third Party Service Providers to serve you the

correct version of the service and provide accurate details about that location for the best possible user experience, e.g. weather details, location access (as part of the Android platform). You may turn this off at any time by going into the device settings or discontinue use of that application.

- **Improving user experience.** Some opt-in features, such as the User Experience Program, allow Xiaomi to analyze data about how users use the mobile phone and MIUI services, so as to improve the user experience, such as sending crash reports.
- **Allowing you to use Security Center.** Information collected may be used for security and system up-keeping functionalities in the Security Center, such as advertising blocker, virus scan, power saver, blocklist, cleaner, etc. Some of these functionalities are operated by Third Party Service Providers. Information (which is not personal information like virus definition lists) is used for virus scan functions.
- **Providing Push Service.** Mi Account ID and IMEI numbers will also be used to provide the Xiaomi push service to evaluate advertising performance and send notifications from MIUI about software updates or new product announcements, including information about sales and promotion. Furthermore, under entrust of selected third party (the data controller of your personal information), the Xiaomi push service may also evaluate advertising performance or send notifications by using your Mi Account ID and IMEI numbers. You consent to our use of your personal information for the purpose of sending you pushing services (whether by messaging within our services, by email or by other means) that offer or advertise our products and services and/or the products and services of selected third parties. You may opt out of this at any time through changing your preferences under “Settings”, or through the selected third party you consent.
- **Verifying user identity.** Xiaomi uses the ECV value to verify the user identity and ensure there is no log-in by hackers or unauthorized persons.
- **Collecting user feedback.** The feedback you choose to provide is valuable in helping Xiaomi make improvements to our services. In order to follow up on the feedback you have chosen to provide, Xiaomi may correspond with you using the personal information that you have provided and keep records.
- **Sending notices.** From time to time, we may use your personal information to send important notices, such as communications about purchases and changes to our terms, conditions, and policies.
- **Conducting promotional activities.** If you enter into a sweepstake, contest, or similar promotion, e.g. via Xiaomi’s Facebook page or other social media platforms, we may use the personal information you provide to administer those programs.
- **Conducting analysis of your device to provide better user experience.** Xiaomi may conduct the hardware or software analysis, so as to further improve the performance of your device.

Direct marketing

- We may use your name, phone number, and email address, Mi Account ID and IMEI number to provide marketing materials to you relating to goods and services of Xiaomi companies and our business partners which offer network, mobile applications and cloud products and services. To provide better user experience, we may recommend above-mentioned products, services and activities based on information about your purchase history, website browsing history, birthday, age, gender, and location. We will only so use your personal data after we obtain your prior explicit consent and involve a clear affirmative action or indication of no objection in accordance with local data protection laws, which may require separate explicit consent. You have the right to opt out of our proposed use of your personal data for direct marketing. If you no longer wish to receive certain types of email communications you may opt-out by following the unsubscribe link located at the bottom of each communication. We will not transfer your personal data to our business partners for use by our business partners in direct marketing.

Cookies and other technologies

- **What information is collected and how we can use them:** Technologies such as cookies, tags, and scripts are used by Xiaomi and our Third Party Service Providers. These technologies are used in analyzing trends, administering the site, tracking users' movements around the website and to gather demographic information about our user base as a whole. We may receive reports based on the use of these technologies by these companies on an individual as well as aggregated basis.
- **Log Files:** As true of most websites, we gather certain information and store it in log files. This information may include Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and/or clickstream data. We do not link this automatically collected data to other information we gather about you.
- **Advertising:** We partner with our Third Party Service Providers to either display advertising on our website or to manage our advertising on other sites. Our Third Party Service Provider may use technologies such as cookies to gather information about your activities on this site and other sites in order to provide you advertising based upon your browsing activities and interests. We will obtain your prior explicit consent and involve a clear affirmative action before providing this advertising service to you. If you wish to not have this information used for the purpose of serving you interest-based ads, you may opt-out by clicking here http://preferences-mgr.truste.com.
- **Mobile Analytics:** Within some of our mobile applications we use mobile analytics software to allow us to better understand the functionality of our Mobile Software on your phone. This software may record information such as how often you use the application, the events that occur within the application, aggregated usage, performance data, and where crashes occur within the application. We do not link the information we store within the analytics software to any personal information you submit within the mobile application.

- **Local Storage – HTML5/Flash:** We use Local Storage Objects (LSOs) such as HTML5 or Flash to store content and preferences. Third parties with whom we partner to provide certain features on our Sites or to display advertising based upon your web browsing activity also use HTML5 or Flash cookies to collect and store information. Various browsers may offer their own management tool for removing HTML5 LSOs. To manage Flash cookies, please click here: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html .

With whom we share your information

We do not sell any personal information to third parties.

We may disclose your personal information on occasion to third parties (as described below) in order to provide the products or services that you have requested.

Disclosure may be made to Third Party Service Providers and affiliated companies listed in this section below. In each case described in this section, you can be assured that Xiaomi will only share your personal information in accordance with your consent. Your consent to Xiaomi will engage sub-processors for the processing of your personal information. You should know that when Xiaomi shares your personal information with a Third Party Service Provider under any circumstance described in this section, Xiaomi will contractually specify that the third party is subject to practices and obligations to comply with applicable local data protection laws. Xiaomi will contractually ensure compliance by any Third Party Service Providers with the privacy standards that apply to them in your home jurisdiction.

Sharing with our group and third party service providers

From time to time, in order to conduct business operations smoothly in providing you with the full capabilities of our products and services, we may disclose your personal information from time to time to other Xiaomi affiliated companies (in communications, social media, technology or cloud businesses), or our third party service providers which are our mailing houses, delivery service providers, telecommunications companies, data centers, data storage facilities, customer service providers, advertising and marketing service providers, agents acting on behalf of Xiaomi, [related corporations, and/or other third parties] (together “Third Party Service Providers”). Such Third Party Service Providers would be processing your personal information on Xiaomi’s behalf or for one or more of the purposes listed above. We may share your IP address with third parties when using certain mobile applications on our device in order to provide you with some of the services you requested. If you no longer wish to allow us to share this information, please contact us at privacy@xiaomi.com.

Sharing with our group’s ecosystem companies

Xiaomi works together with a cool group of companies, which together form the Mi Ecosystem. The Mi Ecosystem companies are independent entities, invested and incubated by Xiaomi, and are experts in their fields. Xiaomi may disclose your personal data to the Mi Ecosystem companies so as to provide you with and improve the exciting products and services (both hardware and software) from the Mi Ecosystem companies. Some of these products and services will still be under the Xiaomi brand, while others may use their own brand. The Mi Ecosystem companies may also share data with Xiaomi from time to time in relation to products and services under the Xiaomi brand and other brands owned by Xiaomi to provide hardware and software services, and to create better functions and user experience. Xiaomi will take appropriate organizational and technical measures to ensure the security of personal data during the process of sharing of information, including but not limited to the encryption of your personal data. If Xiaomi is involved in a merger, acquisition or asset sale of all or a portion of our assets, you will be notified via email and/or a prominent notice on our website, of any changes in ownership, uses of your personal information, and choices you may have regarding your personal information.

Sharing with others

Xiaomi may disclose your personal information without further consent when required under applicable law.

Information not requiring consent

- We may share anonymized information and statistics in aggregate form with third parties for business purposes, for example with advertisers on our website, we may share them trends about the general use of our services, such as the number of customers in certain demographic groups who purchased certain products or who carried out certain transactions.
- For the avoidance of doubt, Xiaomi may collect, use or disclose your personal information without your consent if it is and only to the extent it is allowed explicitly under local data protection laws.

Security safeguards

Xiaomi's security measures

We are committed to ensuring that your personal information is secure. In order to prevent unauthorized access, disclosure or other similar risks, we have put in place reasonable physical, electronic and managerial procedures to safeguard and secure the information we collect on your mobile device and on Xiaomi websites. We will use all reasonable efforts to safeguard your personal information.

For example, when you access your Mi Account, you can choose to use our two-step verification process for better security. When you send or receive data from your Xiaomi device to our servers, we make sure they are encrypted using Secure Sockets Layer ("SSL") and other algorithms.

All your personal information is stored on secure servers that are protected in controlled facilities. We classify your data based on importance and sensitivity, and ensure that your personal information has the highest security level. We make sure that our employees and Third Party Service Providers who access the information to help provide you with our products and services are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet such obligations. We have special access controls for cloud based data storage as well. All in all, we regularly review our information collection, storage and processing practices, including physical security measures, to guard against any unauthorized access and use.

We will take all practicable steps to safeguard your personal information. However, you should be aware that the use of the Internet is not entirely secure, and for this reason we cannot guarantee the security or integrity of any personal information which is transferred from you or to you via the Internet.

We will take upon the personal data breach, notifying the breach to relevant supervisory authority or under some circumstances, notifying the personal data breach to the data subjects by complying with applicable laws, including your local data protection legislation.

What you can do

- You can play your part in safeguarding your personal information by not disclosing your login password or account information to anybody unless such person is duly authorized by you. Whenever you log in as a Mi Account user on Xiaomi websites, particularly on somebody else's computer or on public Internet terminals, you should always log out at the end of your session.
- Xiaomi cannot be held responsible for lapses in security caused by third party accesses to your personal information as a result of your failure to keep your personal information private. Notwithstanding the foregoing, you must notify us immediately if there is any unauthorized use of your account by any other Internet user or any other breach of security.
- Your assistance will help us protect the privacy of your personal information.

Retention policy

Personal information will be held for as long as it is necessary to fulfill the purpose for which it was collected, or as required or permitted by applicable laws. We shall cease to retain personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal information was collected is no longer being served by retention of the personal information. If further processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes according to the applicable laws, the data can be further retained by Xiaomi even if the further processing is incompatible with original purposes.

Accessing other features on your device

Our applications may need access to certain features on your device such as enabling emails to contacts, SMS storage and Wi-Fi network status, as well as other features. This information is used to allow the applications to run on your device and allow you to interact with the applications. At any time you may revoke your permissions by turning these off at the device level or contacting us at privacy@xiaomi.com.

You have control over your personal information

Controlling settings

Xiaomi recognizes that privacy concerns differ from person to person. Therefore, we provide examples of ways Xiaomi makes available for you to choose to restrict the collection, use, disclosure or processing of your personal information and control your privacy settings:

- Toggle on/off for the User Experience Program and Location Access functions;
- Log in and out of the Mi Account;
- Toggle on/off for the Mi Cloud sync functions; and
- Delete any information stored on Mi Cloud through www.mi.com/micloud
- Toggle on/off for other services and functionalities which deal with sensitive or personal information.

You may obtain more details in relation to your device's security status in the MIUI Security Center as well.

If you have previously agreed to us using your personal information for the abovementioned purposes, you may change your mind at any time by writing or emailing us at privacy@xiaomi.com.

Access, update, correct, erase or restrict processing your personal information

- You have the right to request access to and/or correction of any other personal information that we hold about you. When you update your personal information, you will be asked to verify your identity before we proceed with your request. Once we obtain sufficient information to accommodate your request for access to or correction of your personal information, we shall proceed to respond to your request within any timeframe set out under your applicable data protection laws.
- A copy of your personal data collected and processed by us will be provided to you upon your request free of charge. For any extra requests of the same information, we may charge a reasonable fee based on actual administrative costs according to the applicable laws.
- If you would like to request access to your personal data held by us or if you believe any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible at the email address below. Email: privacy@xiaomi.com
- For details relating to the personal information in your Mi Account, you may also access and change them at http://account.mi.com or by logging into your account on your device.

- If you are Europe Union user under General Data Protection Regulation (GDPR), you have the right to obtain from us the erasure of your personal information. We shall consider the grounds regarding your erasure request and take reasonable steps, including technical measures, if the grounds apply to GDPR.
- If you are Europe Union user under GDPR, you have the right to obtain from us the restriction of processing your personal information. We shall consider the grounds regarding your restriction request. If the grounds apply to GDPR, we shall only process your personal information under applicable circumstances in GDPR and inform you before the restriction of processing is lifted.
- If you are Europe Union user under GDPR, you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.
- If you are Europe Union user under GDPR, you have the right to receive your personal information in a structured, commonly used format and transmit the information to another data controller.

Withdrawal of consent

- You may withdraw your consent for the collection, use and/or disclosure of your personal information in our possession or control by submitting a request. This may be done by accessing your Mi Account management center at account.xiaomi.com/pass/del. We will process your request within a reasonable time from when the request was made, and thereafter not collect, use and/or disclose your personal information as per your request.
- Please recognize that your withdrawal of consent could result in certain legal consequences. Depending on the extent of your withdrawal of consent for us to process your personal information, it may mean that you will not be able to enjoy Xiaomi's products and services.

Transfer of personal information outside of your jurisdiction

To the extent that we may need to transfer personal information outside of your jurisdiction, whether to our affiliated companies (which are in the communications, social media, technology and cloud businesses) or Third Party Service Providers, we shall do so in accordance with the applicable laws. In particular, we will ensure that all transfers will be in accordance with requirements under your applicable local data protection laws by putting in place appropriate safeguards. You will have the right to be informed of the appropriate safeguards taken by Xiaomi for this transfer of your personal information.

Xiaomi is a China-headquartered company operating globally. As such, complying with applicable laws, we may transfer your personal data to any subsidiary of the Xiaomi group worldwide when processing that information for the purposes described in this Privacy Policy. We may also transfer your personal data to our third party service providers, who may be located in a country or area outside the area of the European Economic Area (EEA).

Whenever Xiaomi shares personal data originating in the EEA with a third party which may or may not be a Xiaomi entity outside the EEA, we will do so on the basis of EU standard contractual clauses or any other safeguards provided for in the GDPR.

Xiaomi may use overseas facilities operated and controlled by Xiaomi to process or back up your personal information. Currently, Xiaomi has data centers in Beijing, United States, Germany, Russia and Singapore. These overseas jurisdictions may or may not have in place data protection laws which are substantially similar to that in your home jurisdiction. We may transfer to and store your personal information at our overseas facilities. However, this does not change any of our commitments to safeguard your personal information in accordance with this Privacy Policy.

Miscellaneous

Minors

- We consider it the responsibility of parents to monitor their children's use of our products and services. Nevertheless, it is our policy not to require personal information from minors or offer to send any promotional materials to persons in that category.
- Xiaomi does not seek or intend to seek to receive any personal information from minors. Should a parent or guardian have reasons to believe that a minor has provided Xiaomi with personal information without their prior consent, please contact us to ensure that the personal information is removed and the minor unsubscribes from any of the applicable Xiaomi services.

Order of precedence

If you have agreed to our applicable User Agreements, in the event of inconsistency between such User Agreements and this Privacy Policy, such User Agreements shall prevail.

Updates to the privacy policy

We keep our Privacy Policy under regular review and may update this privacy policy to reflect changes to our information practices. If we make material changes to our Privacy Policy, we will notify you by email (sent to the e-mail address specified in your account) or post the changes on all the Xiaomi websites or through our mobile devices, so that you may be aware of the information we collect and how we use it. Such changes to our Privacy Policy shall apply from the effective date as set out in the notice or on the website. We encourage you to periodically review this page for the latest information on our privacy practices. Your continued use of products and services on the websites, mobile phones and/or any other device will be taken as acceptance of the updated Privacy Policy. We will seek your fresh consent before we collect more personal information from you or when we wish to use or disclose your personal information for new purposes.

Do I have to agree to any third party terms and conditions?

Our Privacy Policy does not apply to products and services offered by a third party. Xiaomi products and services may include third parties' products, services and links to third parties' websites. When you use such products or services, they may collect your information too. For this reason, we strongly suggest that you read the third party's privacy policy as you have taken time to read ours. We are not responsible for and cannot control how third parties use personal information which they collect from you. Our Privacy Policy does not apply to other sites linked from our services.

Here are third party terms and privacy policies that apply when you use these specific products:

- By using PayPal or other third party check-out services to finalize and pay for your order, you are agreeing to the third party check-out service provider's privacy policy will apply to the information you provide on the their website.
- By using the Virus Scan feature in the MIUI Security Center, you are agreeing to one of the following three terms based on your choice of service.
    - Avast Privacy and Information Security Policy: https://www.avast.com/privacy-policy
    - License Agreement for AVL SDK for Mobile: http://co.avlsec.com/License.en.html?l=en
    - Tencent's Terms of Service: http://wesecure.qq.com/termsofservice.jsp
- By using the Cleaner feature in MIUI's Security Center, you are agreeing to one of the following two terms based on your choice of service.
    - Cheetah Mobile's Privacy Policy: http://www.cmcm.com/protocol/cleanmaster/privacy-for-sdk.html
    - Tencent's Terms of Service: http://wesecure.qq.com/termsofservice.jsp
- By using the advertising services in several specific applications in MIUI, you are agreeing to one of the following two terms based on your choice of service.
    - Google's Privacy Policy: https://policies.google.com/
    - Facebook's Privacy Policy: https://www.facebook.com/about/privacy/update?ref=old_policy
- By using the Google Input Method, you are agreeing to Google's terms: http://www.google.com/policies/privacy
- By using the SwiftKey Input Method, you are agreeing to SwiftKey's terms: http://swiftkey.com/en/privacy

Social media (features) and widgets

Our websites include social media features, such as the Facebook Like button and Widgets, such as the Share this button or interactive mini-programs that run on our site. These features may collect your IP address, which page you are visiting on our site, and may set a cookie to enable the Feature to function properly. Social media features and Widgets are either hosted by a third party or hosted directly on our websites. Your interactions with these Features are governed by the privacy policy of the company providing it.

Single sign-on

Depending on your jurisdiction, you may be able to log in to our website using sign-on services such as Facebook Connect or an Open ID provider. These services will authenticate your identity, provide you the option to share certain personal information (such as your name and email address) with us, and to pre-populate our sign up form. Services like Facebook Connect give you the option to post information about your activities on this website to your profile page to share with others within your network.

About our systematic approach to manage your personal information

If you are Europe Union user under GDPR, Xiaomi will provide systematic approach to manage personal data deeply engages our people, management processes and information systems by applying a risk management methodology. According to the GDPR, for instance, (1) Xiaomi set up a Data Protection Officer (DPO) in charge the data protection, and the contact of DPO is dpo@xiaomi.com; (2) procedure like data protection impact assessment (DPIA).

Contact us

If you have any comments or questions about this Privacy Policy or any questions relating to Xiaomi's collection, use or disclosure of your personal information, please contact our Data Protection Officer at the address below referencing "Privacy Policy":

Xiaomi Singapore Pte. Ltd.
20 Cross Street, China Court #02-12
Singapore 048422
Email: privacy@xiaomi.com

Thank you for taking the time to understand our Privacy Policy!

What's new to you

We have made several major edits throughout the "Privacy Policy" as follows:

- We updated the types of personal information that we collected and the purposes of collecting such information. For example, we collected hardware usage information to conduct statistical analysis and optimize the performance of your devices.

- By complying with GDPR and providing better data privacy protection, we updated the relevant content about users' rights under GDPR, and how we process the personal information for our Europe Union users. We also described our data privacy management method additionally.
- We updated the relevant content of third parties' products and services which may be involved during the use of our products and services.

Google[741]

An updated version of our Privacy Policy takes effect on May 25, 2018.

Privacy Policy

Last modified: December 18, 2017 (view archived versions)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices – and if you have any questions contact us.

Information we collect

We collect information to provide better services to all of our users – from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like.

We collect information in the following ways:

- **Information you give us.** For example, many of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card to store with your account. If you want to take full advantage of the sharing features we offer, we might also ask you to create a publicly visible Google Profile, which may include your name and photo.

[741] "Welcome to the Google Privacy Policy," Google LLC.

- **Information we get from your use of our services.** We collect information about the services that you use and how you use them, like when you watch a video on YouTube, visit a website that uses our advertising services, or view and interact with our ads and content. This information includes:
    - Device information

      We collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number). Google may associate your device identifiers or phone number with your Google Account.
    - **Log information**

      When you use our services or view content provided by Google, we automatically collect and store certain information in server logs. This includes:
        - details of how you used our service, such as your search queries.
        - telephony log information like your phone number, calling-party number, forwarding numbers, time and date of calls, duration of calls, SMS routing information and types of calls.
        - Internet protocol address.
        - device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
        - cookies that may uniquely identify your browser or your Google Account.
    - **Location information**

      When you use Google services, we may collect and process information about your actual location. We use various technologies to determine location, including IP address, GPS, and other sensors that may, for example, provide Google with information on nearby devices, Wi-Fi access points and cell towers.
    - **Unique application numbers**

      Certain services include a unique application number. This number and information about your installation (for example, the operating system type and application version number) may be sent to Google when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.
    - **Local storage**

      We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.
    - **Cookies and similar technologies**

> We and our partners use various technologies to collect and store information when you visit a Google service, and this may include using cookies or similar technologies to identify your browser or device. We also use these technologies to collect and store information when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites. Our Google Analytics product helps businesses and site owners analyze the traffic to their websites and apps. When used in conjunction with our advertising services, such as those using the DoubleClick cookie, Google Analytics information is linked, by the Google Analytics customer or by Google, using Google technology, with information about visits to multiple sites.

Information we collect when you are signed in to Google, in addition to information we obtain about you from partners, may be associated with your Google Account. When information is associated with your Google Account, we treat it as personal information. For more information about how you can access, manage or delete information that is associated with your Google Account, visit the Transparency and choice section of this policy.

How we use information we collect

We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.

We may use the name you provide for your Google Profile across all of the services we offer that require a Google Account. In addition, we may replace past names associated with your Google Account so that you are represented consistently across all our services. If other users already have your email, or other information that identifies you, we may show them your publicly visible Google Profile information, such as your name and photo.

If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account.

When you contact Google, we keep a record of your communication to help solve any issues you might be facing. We may use your email address to inform you about our services, such as letting you know about upcoming changes or improvements.

We use information collected from cookies and other technologies, like pixel tags, to improve your user experience and the overall quality of our services. One of the products we use to do this on our own services is Google Analytics. For example, by saving your language preferences, we'll be able to have our services appear in the language you prefer. When showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.

We may combine personal information from one service with information, including personal information, from other Google services – for example to make it easier to share things with people you know. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.

Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.

Transparency and choice

People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:

- Review and update your Google activity controls to decide what types of data, such as videos you've watched on YouTube or past searches, you would like saved with your account when you use Google services. You can also visit these controls to manage whether certain activity is stored in a cookie or similar technology on your device when you use our services while signed-out of your account.
- Review and control certain types of information tied to your Google Account by using Google Dashboard.
- View and edit your preferences about the Google ads shown to you on Google and across the web, such as which categories might interest you, using Ads Settings. You can also visit that page to opt out of certain Google advertising services.
- Adjust how the Profile associated with your Google Account appears to others.
- Control who you share information with through your Google Account.
- Take information associated with your Google Account out of many of our services.
- Choose whether your Profile name and Profile photo appear in shared endorsements that appear in ads.

You may also set your browser to block all cookies, including cookies associated with our services, or to indicate when a cookie is being set by us. However, it's important to remember that many of our services may not function properly if your cookies are disabled. For example, we may not remember your language preferences.

Information you share

Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.

Accessing and updating your personal information

Whenever you use our services, we aim to provide you with access to your personal information. If that information is wrong, we strive to give you ways to update it quickly or to delete it – unless we have to keep that information for legitimate business or legal purposes.

We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

- **With your consent**

  We will share personal information with companies, organizations or individuals outside of Google when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

- **With domain administrators**

  If your Google Account is managed for you by a domain administrator (for example, for G Suite users) then your domain administrator and resellers who provide user support to your organization will have access to your Google Account information (including your email and other data). Your domain administrator may be able to:

  - view statistics regarding your account, like statistics regarding applications you install.
  - change your account password.
  - suspend or terminate your account access.
  - access or retain information stored as part of your account.
  - receive your account information in order to satisfy applicable law, regulation, legal process or enforceable governmental request.
  - restrict your ability to delete or edit information or privacy settings.

  Please refer to your domain administrator's privacy policy for more information.

- **For external processing**

  We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

- **For legal reasons**

We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

- meet any applicable law, regulation, legal process or enforceable governmental request.
- enforce applicable Terms of Service, including investigation of potential violations.
- detect, prevent, or otherwise address fraud, security or technical issues.
- protect against harm to the rights, property or safety of Google, our users or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers or connected sites. For example, we may share information publicly to show trends about the general use of our services.

If Google is involved in a merger, acquisition or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

Information security

We work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services using SSL.
- We offer you two step verification when you access your Google Account, and a Safe Browsing feature in Google Chrome.
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

When this Privacy Policy applies

Our Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, services Google provides on Android devices, and services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include Google services, or other sites linked from our services. Our Privacy Policy does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

Compliance and cooperation with regulatory authorities

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks, including the EU-US and Swiss-US Privacy Shield Frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

Changes

Our Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of privacy policy changes). We will also keep prior versions of this Privacy Policy in an archive for your review.

Specific product practices

The following notices explain specific privacy practices with respect to certain Google products and services that you may use:

- Chrome and Chrome OS
- Play Books
- Payments
- Fiber
- Project Fi
- G Suite for Education
- YouTube Kids
- Google Accounts Managed with Family Link

For more information about some of our most popular services, you can visit the Google Product Privacy Guide.

Other useful privacy and security related materials

Further useful privacy and security related materials can be found through Google's policies and principles pages, including:

- Information about our technologies and principles, which includes, among other things, more information on
    - how Google uses cookies.

  - technologies we use for advertising.
  - how we recognize patterns like faces.
- A page that explains what data is shared with Google when you visit websites that use our advertising, analytics and social products.
- The Privacy Checkup tool, which makes it easy to review your key privacy settings.
- Google's safety center, which provides information on how to stay safe and secure online.

Example

Google Analytics is based on first-party cookies. Data generated through Google Analytics can be linked, by the Google Analytics customer or by Google, using Google technology, to third-party cookies, related to visits to other websites, for instance when an advertiser wants to use its Google Analytics data to create more relevant ads, or to further analyze its traffic.

Learn more.

Apple[742]

Privacy Policy

The Apple Privacy Policy was updated on January 19, 2018.

Your privacy is important to Apple. So we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your information. Please take a moment to familiarize yourself with our privacy practices and let us know if you have any questions.

Your California Privacy Disclosures
Information Regarding Commercial Electronic Messages in Canada

Collection and Use of Personal Information

Personal information is data that can be used to identify or contact a single person.

You may be asked to provide your personal information anytime you are in contact with Apple or an Apple affiliated company. Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising. You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have.

Here are some examples of the types of personal information Apple may collect and how we may use it:

[742] "Privacy Policy," Apple Inc., accessed May 14, 2018, https://www.apple.com/legal/privacy/en-ww

What personal information we collect

- When you create an Apple ID, apply for commercial credit, purchase a product, download a software update, register for a class at an Apple Retail Store, contact us or participate in an online survey, we may collect a variety of information, including your name, mailing address, phone number, email address, contact preferences, and credit card information.
- When you share your content with family and friends using Apple products, send gift certificates and products, or invite others to participate in Apple services or forums, Apple may collect the information you provide about those people such as name, mailing address, email address, and phone number. Apple will use such information to fulfill your requests, provide the relevant product or service, or for anti-fraud purposes.
- In certain jurisdictions, we may ask for a government issued ID in limited circumstances including when setting up a wireless account and activating your device, for the purpose of extending commercial credit, managing reservations, or as required by law.

How we use your personal information

- The personal information we collect allows us to keep you posted on Apple's latest product announcements, software updates, and upcoming events. If you don't want to be on our mailing list, you can opt out anytime by updating your preferences.
- We also use personal information to help us create, develop, operate, deliver, and improve our products, services, content and advertising, and for loss prevention and anti-fraud purposes.
- We may use your personal information, including date of birth, to verify identity, assist with identification of users, and to determine appropriate services. For example, we may use date of birth to determine the age of Apple ID account holders.
- From time to time, we may use your personal information to send important notices, such as communications about purchases and changes to our terms, conditions, and policies. Because this information is important to your interaction with Apple, you may not opt out of receiving these communications.
- We may also use personal information for internal purposes such as auditing, data analysis, and research to improve Apple's products, services, and customer communications.
- If you enter into a sweepstake, contest, or similar promotion we may use the information you provide to administer those programs.

Collection and Use of Non-Personal Information

We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

- We may collect information such as occupation, language, zip code, area code, unique device identifier, referrer URL, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.
- We may collect information regarding customer activities on our website, iCloud services, our iTunes Store, App Store, Mac App Store, App Store for Apple TV and iBooks Stores and from our other products and services. This information is aggregated and used to help us provide more useful information to our customers and to understand which parts of our website, products, and services are of most interest. Aggregated data is considered non-personal information for the purposes of this Privacy Policy.
- We may collect and store details of how you use our services, including search queries. This information may be used to improve the relevancy of results provided by our services. Except in limited instances to ensure quality of our services over the Internet, such information will not be associated with your IP address.
- With your explicit consent, we may collect data about how you use your device and applications in order to help app developers improve their apps.

If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.

Cookies and Other Technologies

Apple’s websites, online services, interactive applications, email messages, and advertisements may use "cookies" and other technologies such as pixel tags and web beacons. These technologies help us better understand user behavior, tell us which parts of our websites people have visited, and facilitate and measure the effectiveness of advertisements and web searches. We treat information collected by cookies and other technologies as non-personal information. However, to the extent that Internet Protocol (IP) addresses or similar identifiers are considered personal information by local law, we also treat these identifiers as personal information. Similarly, to the extent that non-personal information is combined with personal information, we treat the combined information as personal information for the purposes of this Privacy Policy.

Ads that are delivered by Apple’s advertising platform may appear in Apple News and in the App Store. If you do not wish to receive ads targeted to your interests from Apple's advertising platform, you can choose to enable Limit Ad Tracking, which will opt your Apple ID out of receiving such ads regardless of what device you are using. If you enable Limit Ad Tracking on your mobile device, third-party apps cannot use the Advertising Identifier, a non-personal device identifier, to serve you targeted ads. You may still see ads in the App Store or News based on context like your search query or the channel you are reading. In third-party apps, you may see ads based on other information.

Apple and our partners also use cookies and other technologies to remember personal information when you use our website, online services, and applications. Our goal in these cases is to make your experience with Apple more convenient and personal. For example, knowing your first name lets us welcome you the next time you visit the Apple Online Store. Knowing your country and language − and if you are an educator, your school − helps us provide a customized and more useful shopping experience. Knowing someone using your computer or device has shopped for a certain product or used a particular service helps us make our advertising and email communications more relevant to your interests. And knowing your contact information, hardware identifiers, and information about your computer or device helps us personalize your operating system, set up your iCloud service, and provide you with better customer service.

If you want to disable cookies and you're using the Safari web browser, go to Safari preferences and then to the privacy pane to manage your preferences. On your Apple mobile device, go to Settings, then Safari, scroll down to the Privacy & Security section, and tap on "Block Cookies" to manage your preferences. For other browsers, check with your provider to find out how to disable cookies. Please note that certain features of the Apple website will not be available once cookies are disabled.

As is true of most internet services, we gather some information automatically and store it in log files. This information includes Internet Protocol (IP) addresses, browser type and language, Internet service provider (ISP), referring and exit websites and applications, operating system, date/time stamp, and clickstream data.

We use this information to understand and analyze trends, to administer the site, to learn about user behavior on the site, to improve our product and services, and to gather demographic information about our user base as a whole. Apple may use this information in our marketing and advertising services.

In some of our email messages, we use a "click-through URL" linked to content on the Apple website. When customers click one of these URLs, they pass through a separate web server before arriving at the destination page on our website. We track this click-through data to help us determine interest in particular topics and measure the effectiveness of our customer communications. If you prefer not to be tracked in this way, you should not click text or graphic links in the email messages.

Pixel tags enable us to send email messages in a format customers can read, and they tell us whether mail has been opened. We may use this information to reduce or eliminate messages sent to customers.

Disclosure to Third Parties

At times Apple may make certain personal information available to strategic partners that work with Apple to provide products and services, or that help Apple market to customers. For example, when you purchase and activate your iPhone, you authorize Apple and your carrier to exchange the information you provide during the activation process to carry out service. If you are approved for service, your account will be governed by Apple and your carrier's respective privacy policies. Personal information will only be shared by Apple to provide or improve our products, services and advertising; it will not be shared with third parties for their marketing purposes.

Service Providers

Apple shares personal information with companies who provide services such as information processing, extending credit, fulfilling customer orders, delivering products to you, managing and enhancing customer data, providing customer service, assessing your interest in our products and services, and conducting customer research or satisfaction surveys. These companies are obligated to protect your information and may be located wherever Apple operates.

Others

It may be necessary − by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence − for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.

We may also disclose information about you if we determine that disclosure is reasonably necessary to enforce our terms and conditions or protect our operations or users. Additionally, in the event of a reorganization, merger, or sale we may transfer any and all personal information we collect to the relevant third party.

Protection of Personal Information

Apple takes the security of your personal information very seriously. Apple online services such as the Apple Online Store and iTunes Store protect your personal information during transit using encryption such as Transport Layer Security (TLS). When your personal data is stored by Apple, we use computer systems with limited access housed in facilities using physical security measures. iCloud data is stored in encrypted form including when we utilize third-party storage.

When you use some Apple products, services, or applications or post on an Apple forum, chat room, or social networking service, the personal information and content you share is visible to other users and can be read, collected, or used by them. You are responsible for the personal information you choose to share or submit in these instances. For example, if you list your name and email address in a forum posting, that information is public. Please take care when using these features.

If you or anyone else using Family Sharing logs on to a device that is owned by a third party, any information shared within your Family—including calendar, location, photos, and iTunes purchases—may be downloaded on to that third-party device thereby disclosing any such shared information. [See About Family Sharing for more information.]

Integrity and Retention of Personal Information

Apple makes it easy for you to keep your personal information accurate, complete, and up to date. We will retain your personal information for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law.

Access to Personal Information

You can help ensure that your contact information and preferences are accurate, complete, and up to date by logging in to your account at https://appleid.apple.com/. For other personal information we hold, we will provide you with access (including a copy) for any purpose including to request that we correct the data if it is inaccurate or delete the data if Apple is not required to retain it by law or for legitimate business purposes. We may decline to process requests that are frivolous/vexatious, jeopardize the privacy of others, are extremely impractical, or for which access is not otherwise required by local law. Access, correction, or deletion requests can be made through the regional Privacy Contact Form.

Children & Education

We understand the importance of taking extra precautions to protect the privacy and safety of children using Apple products and services. Children under the age of 13, or equivalent minimum age in the relevant jurisdiction, are not permitted to create their own Apple IDs, unless their parent provided verifiable consent or as part of the child account creation process in Family Sharing or they have obtained a Managed Apple ID account (where available) through their school. For example, a parent must review the Apple ID and Family Sharing Disclosure and agree to the Consent to Apple's Collection, Use and Disclosure of Your Child's Information; and the iTunes Store Terms and Conditions, before they can begin the Apple ID account creation process for their child. In addition, schools that participate in Apple School Manager and have reviewed and consented to the Managed Apple IDs for Students Disclosure may create Managed Apple IDs for students. The Managed Apple IDs for Students Disclosure describes how Apple handles student information and supplements Apple's Privacy Policy. Learn more about Family Sharing, the Managed Apple IDs and Restrictions for children's accounts.

If we learn that we have collected the personal information of a child under 13, or equivalent minimum age depending on jurisdiction, outside the above circumstances we will take steps to delete the information as soon as possible.

If at any time a parent needs to access, correct, or delete data associated with their Family Sharing account or child's Apple ID, they may contact us through our Privacy Contact Form.

Or by using the contact information here.

Location-Based Services

To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. Where available, location-based services may use GPS, Bluetooth, and your IP Address, along with crowd-sourced Wi-Fi hotspot and cell tower locations, and other technologies to determine your devices' approximate location. Unless you provide consent, this location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, your device may share its geographic location with application providers when you opt in to their location services.

Some location-based services offered by Apple, such as the "Find My iPhone" feature, require your personal information for the feature to work.

Third-Party Sites and Services

Apple websites, products, applications, and services may contain links to third-party websites, products, and services. Our products and services may also use or offer products or services from third parties − for example, a third-party iPhone app.

Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.

If you purchase a subscription in a third party app or within News, we create a Subscriber ID that is unique to you and the developer or publisher which we use to provide reports to the developer or publisher that include information about the subscription you purchased, and your country of residence. If you cancel all of your subscriptions with a particular developer or publisher, the Subscriber ID will reset after 180 days if you do not resubscribe. This information is provided to developers so that they can understand the performance of their subscriptions.

International Users

All the information you provide may be transferred or accessed by entities around the world as described in this Privacy Policy. Personal information, relating to Apple services, regarding individuals who reside in a member state of the European Economic Area and Switzerland is controlled by Apple Distribution International in Ireland, and processed on its behalf by Apple Inc. Apple uses approved Model Contractual Clauses for the international transfer of personal information collected in the European Economic Area and Switzerland. Apple, as a global company, has a number of legal entities in different jurisdictions which are responsible for the personal information which they collect and which is processed on their behalf by Apple Inc. For example, point of sale information in our Retail entities outside the U.S. is controlled by our individual Retail entities in each country. Apple, Online Store and iTunes related personal information may also be controlled by legal entities outside the U.S. as reflected in the terms of each service.

Apple abides by the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules System. The APEC CBPR system provides a framework for organizations to ensure protection of personal information transferred among participating APEC economies. To learn more about the APEC Certification and Dispute Resolution, please click on the TRUSTe seal.

Our Companywide Commitment to Your Privacy

To make sure your personal information is secure, we communicate our privacy and security guidelines to Apple employees and strictly enforce privacy safeguards within the company.

Privacy Questions

If you have any questions or concerns about Apple's Privacy Policy or data processing or if you would like to make a complaint about a possible breach of local privacy laws, please contact us. You can always contact us by phone at the relevant Apple Support number for your country.

When a privacy question or access/download request is received we have a dedicated team which triages the contacts and seeks to address the specific concern or query which you are seeking to raise. Where your issue may be more substantive in nature, more information may be sought from you. All such substantive contacts receive a response. If you are unsatisfied with the reply received, you may refer your complaint to the relevant regulator in your jurisdiction. If you ask us, we will endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances.

Apple may update its Privacy Policy from time to time. When we change the policy in a material way, a notice will be posted on our website along with the updated Privacy Policy.

Apple Inc. 1 Infinite Loop, Cupertino, California, USA, 95014