Stanford | Geopolitics, Technology, and Governance
*Freeman Spogli Institute*

DIGICHINA

# Mapping U.S.–China Data De-Risking

*Accumulating barriers and safeguards for data transfers*

BY
Samm Sacks
Yan Luo
Graham Webster

February 29, 2024

digichina.stanford.edu

# Introduction

As concerns over data security and privacy collide with geopolitics, policymakers in Washington and Beijing are confronting questions about how to govern data flows between their two countries and beyond. The Internet made moving data of all kinds across borders smooth, simple, and dynamic, bringing both huge benefits and novel risks. Now, with large-scale data resources both fueling advances in artificial intelligence (AI) and creating new vulnerabilities, controlling data has become one of the central elements of the U.S.–China technology conflict.

Unprecedented policy moves are in the works to meet the moment. On February 28, 2024, the Biden Administration issued an executive order (EO) and a proposed rule issued by the Justice Department that for the first time invoke national security to prohibit or require licenses for transferring certain categories and amounts of U.S. data to China and other countries of concern. U.S. policymakers have emphasized that the executive action is intended to narrowly address a specific national security risk focused on data brokers and bulk sales of sensitive types of data, a risk that has not previously been addressed in a comprehensive manner. As the details and scope of the regulations take shape, the fact remains that neither the United States nor China has landed on a long-term answer to concerns in both countries over access to and control over data at a time of heightened mutual suspicion.

Government officials and private sector actors in both countries are debating a range of questions, from what it means to own data in an era when so much of it is collected, to how to safeguard it while still reaping economic benefits. Moreover, deepening distrust between the United States and China has piled

national security and competitiveness concerns atop unresolved questions about a person's rights over data about them and the ethics of data stockpiling by governments and large firms. This array of trade-offs and unresolved questions has not, however, prevented the two governments from making moves to control or shape the data ecosystem.

## *Data amidst U.S.–China friction*

In August 2020, DigiChina published Mapping US–China Technology Decoupling—a snapshot of measures that had already been taken in Washington and Beijing with the effect of unwinding interdependence. That mapping exercise identified actions taken by both governments to separate technology systems across categories including export controls, data, supply chains, encryption, financial untangling, and travel. This update to our 2020 map focuses specifically on actions by both sides affecting data handling and cross-border data flows. It adopts the framing term "de-risking," following the Biden administration's embrace of the phrase as a way to describe its goals as short of complete "decoupling."

Over several months, we compiled a wide array of regulatory shifts that either restrict data flows or stand poised to do so if officials see a need from a national security perspective. In Washington, executive branch actions and legislation introduced in Congress would create broad authorities to review, prohibit, and impose mitigation measures to prevent transfers of sensitive personal or other data to China. Rules on data brokers and other transfers introduced this week are not final, and a Commerce Department supply chain rule (see entries on "ICTS" below) has not been fully implemented. As a result, for now, reviews by the Committee on Foreign Investment in the United States (CFIUS) and the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (known as Team Telecom) remain the only pathways for the U.S. government to address national security concerns involving transferring sensitive data abroad. The current U.S. approach to protecting data from foreign governments of concern thus for now still relies on a case-by-case review and only takes place where CFIUS or Team Telecom has jurisdiction over a transaction. The new EO marks a departure from this

*Acknowledgements: The authors are grateful for the research support of Tabatha Anderson. We thank Martin Chorzempa, Jamie Horsley, Alexa Lee, and Patrick Lozada for taking the time to comment drafts or sections thereof. All errors are our own.*

situation, creating a broader approach to regulating data flows involving countries of concern.

The Chinese government also has inserted itself into the data flow between the United States and China. After many iterations of draft regulations and multiple rounds of public consultations, in September 2022, the government finally implemented an administrative process to review data transfers through government security assessments that, like the new U.S. rule, come into play for certain volumes and kinds of data. That process currently requires government review and approval for an entity in China to transfer the personal data of 1 million or more users, or "important data" that may impact national security, out of the country. Companies that are transferring less data or otherwise do not trigger the security assessment requirement can rely on a less burdensome "standard contract" filing to ensure their data transfers are compliant.

## *Moving data, moving target*

The landscape in both countries is evolving and in most cases has not been enacted or implemented to its fullest possible extent. For evidence that both countries' regimes are in motion, look no further than the second half of 2023. In China, where the details of the regime regulating data transfers out of the country remained murky, the Cyberspace Administration of China (CAC) in September published a new draft regulation that marked a policy shift from the security assessment system described above, which had proved burdensome since it was finalized a year earlier. If implemented, the revision would exempt the majority of companies that transfer limited data for everyday business operations from mandatory security assessments before sending data out of the country. This would remove a time-consuming process and major regulatory risks that had beset a wide range of data transfers necessary for doing business—handling human resources data, for example. The policy change would leave it to the government to specify specific types of data that require reviews before transfer because of national security concerns, which of course leaves plenty of room for further restrictions. Still, it would represent a relaxation of cross-border data barriers.

Meanwhile, roughly a month after the Chinese recalibration, the Office of the United States Trade Representative (USTR) announced that the United States was withdrawing its support in a World Trade Organization (WTO) negotiation for provisions that would favor free data flows and prohibit forced data localization. USTR Spokesperson Sam Michal explained that the shift was designed to leave room for unresolved policy debates at home, saying the prior U.S. positions

"might prejudice or hinder those domestic policy considerations." USTR's decision sparked fierce responses from members of Congress, who argued that it undermined longstanding U.S. commitments and efforts across multiple agencies to promote free data flows. The White House said it stood by its "support for the trusted free flow of data and an open Internet," and that "robust discussion" among perspectives "that are not the same" will continue in the government.

Amid internal debate, USTR's action signaled a shift in the U.S. approach consistent with the direction of this week's data security EO, which for the first time will restrict some data flows to specific destinations. International trade agreements do allow for national security exceptions, so the USTR action was not necessary as a precondition for the EO. Yet taken together, the USTR shift, the data security EO, and Commerce Department requirements for cloud service providers to verify the identity of foreign customers reveal a broader pattern in which national security is invoked to deny access to certain countries, as governments increasingly view data flows as a vulnerability in an era of competition.

The United States and China have long stood far apart on data controls, with China decades into developing inbound barriers in the form of the Great Firewall and years into crafting outbound controls to protect national security, and the United States traditionally a vocal advocate for Internet freedom and free flows of data across borders. These two recent developments show that, while still far apart, reckoning with data's role in society and the economy can sometimes mean they take a step or two toward one another. Beijing regulators seemingly found that their security-motivated efforts to scrutinize all data transfers indiscriminately were having unintended negative consequences on the growth of the economy in general and on foreign investment in particular, and some in Washington apparently believe an ideological commitment to maximally free flows could be a barrier to mitigating data harms. Both sides also appear to be seeking to carve out space to allow data flows in areas deemed less sensitive to national security. At the center of this moment of slight convergence is work on both sides to figure out which forms and uses of data might have national security implications, and how to manage those risks. If nothing else, the two governments share a wariness of each other (among others around the world) and a determination not to let data be their downfall.

## *Mapping data de-risking*

What follows is a compilation of major policy developments affecting cross-border data flows, first from Washington and second from Beijing. This is a selective list, focusing on the most consequential policy moves or proposals and omitting initiatives overtaken by events or without significant momentum. Still, it demonstrates the breadth and complexity of emerging barriers to cross-border data transfers between the United States and China.

# U.S. Policy Developments

FEBRUARY 2024

EO on Bulk Sensitive Personal and Other Data Issued

- Status: Notice of proposed rulemaking issued for public comment.

**WHAT HAPPENED:** The Biden administration issues the Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern and a Department of Justice advance notice of proposed rulemaking (ANPRM). The proposed rules would regulate data transactions between U.S. persons and countries of concern, including China. It defines six categories of sensitive data at "bulk thresholds" subject to regulation: (1) specifically listed categories and combinations of personal identifiers (not all personally identifiable information); (2) precise geolocation data; (3) biometric identifiers; (4) human genomic data; (5) personal health data; and (6) personal financial data. The rules also apply new controls to two kinds of government-related data (geolocation data in certain areas and personal data linkable to military, intelligence, and other kinds of government personnel). Some classes of transactions would be prohibited entirely while others would be prohibited unless they comply with additional security requirements. Prohibited transactions include those with data brokers and with bulk human genomic data or biospecimens.

**WHAT IT MEANS:** These actions represent a shift in the U.S. approach to data policy by creating an authority to review, restrict, and potentially prohibit transfers of Americans' data to specific destinations for the first time. Despite stated goals for the program to be carefully calibrated to address specific threats, the reach and complexity of the ANPRM creates significant uncertainty regarding the potentially broad scope of restricted transactions and the accompanying licensing regime. Outstanding questions remain regarding many factors, including: whether people who are not citizens of a country-of-concern would be restricted because of physical presence in such a country; the order's handling of undersea cables and data centers abroad; and whether the measures would be effective in addressing sophisticated threat actors.

JANUARY 2024

Proposed Rule Would Add Know-Your-Customer Requirements for Cloud Providers

- Open for public comment.

**WHAT HAPPENED:** The Commerce Department's Bureau of Industry & Security (BIS) issues a proposed rule (comment period through April 29, 2024) that would require U.S. Infrastructure-as-a-Service (IaaS) providers and foreign resellers of those services to verify the identity of foreign customers (also referred to as a know-your-customer program or Customer Identification Program). The rule states, "IaaS products offer customers the ability to run software and store data on servers offered for rent or lease," and frames the rationale for the rule as aiming to address threats to U.S. national security in a context where "[f]oreign malicious cyber actors have utilized U.S. IaaS products to commit intellectual property and sensitive data theft." The rule would also require cloud providers to report to the Commerce Department whenever a foreign person "transacts with them to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity." It proposes a definition for AI models deemed dangerous based on certain technical conditions. The proposed rule implements two EOs: Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities (January 2021) and Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 2023).

**WHAT IT MEANS:** The proposed rules aim in part to close a loophole in export controls on advanced semiconductors to China to prevent Chinese companies from circumventing restrictions by remotely accessing infrastructure to train large models. Taken together with other recent actions (the USTR's shift of position at the WTO, the new EO restricting bulk data flows to countries of concern, etc.), these IaaS rules signal a shift underway toward restrictions on services and data based on ties or proximity to foreign governments or firms.

JUNE 2023

Final ICTS Rule Published

- Status: In effect; little implementation so far.

**WHAT HAPPENED:** The Department of Commerce publishes the Final Rule on Securing the Information and Communications Technology and Services (ICTS) Supply Chain. The rule implements the June 2021 Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries.

**WHAT IT MEANS:** Compared with the Interim Final Rule (see January 2021 below), the final rule narrows the scope of covered transactions by specifying that ICTS under the jurisdiction or direction of a foreign adversary, not under its "coercive influence," will be the focus of reviews. By removing "coercive influence," the rule eliminates what could have been a source of uncertainty as to the intended targets of the review, suggesting the Commerce Department may focus reviews on companies headquartered in China. Doing so would limit the number of transactions subject to scrutiny, which had been an earlier source of criticism from U.S. industry. Further developments are expected; for example, in February 2024, Commerce begins an inquiry process into national security risks of connected vehicles.

MARCH 2023

Protecting Military Service Members' Data Act Introduced

- Status: Not passed.

**WHAT HAPPENED:** The Protecting Military Service Members' Data Act, introduced by Senators Elizabeth Warren (D-Mass.), Bill Cassidy (R-La.), and Marco Rubio (R-Fla.) would "prohibit data brokers from selling, reselling, trading, licensing, or otherwise providing for consideration lists of military servicemembers to a covered nation." It has been referred to committee without advancing.

**WHAT IT MEANS:** The proposed legislation aims to close off what some view as a significant pathway for the Chinese government and others to access data about U.S. citizens on open, commercial markets. Advocates for this approach argue that even if certain platforms owned or under the influence of a "foreign adversary" were to be banned or restricted from handling this data, it is still accessible to third countries through data broker sales.

MARCH 2023

RESTRICT Act Introduced

- Status: Not passed.

**WHAT HAPPENED:** Senator Mark Warner (D-Va.) introduces the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act. The legislation would require the Secretary of Commerce to establish procedures to identify, deter, disrupt, prevent, prohibit, and mitigate risks involving ICT transactions in which any foreign adversary has any interest. It has not been enacted.

**WHAT IT MEANS:** The RESTRICT Act never advanced amid criticism from all sides, with some arguing that it would violate the First Amendment and give the Executive Branch too much power, and others arguing it would be too weak.

SEPTEMBER 2022

EO Highlights Data Risks for CFIUS

- Status: In effect.

**WHAT HAPPENED:** President Joe Biden issues the "Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States." The EO elaborates on existing authorities assigned to CFIUS detailing national security concerns surrounding sensitive data and aggregation of large datasets.

**WHAT IT MEANS:** As one of us wrote previously, "These policy statements suggest that U.S. policymakers' concerns go beyond the risk posed by Beijing's access to individual datasets held by one company or platform. Instead, the concern also applies to how combining individual company data with other commercial and proprietary data sets could compromise U.S. national security."

JUNE 2021

EO on 'Protecting Americans' Sensitive Data' Issued

- Status: In effect.

**WHAT HAPPENED:** Biden issues the Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, which outlines a framework for expanding on the May 2019 ICT EO. The new order revokes the mandates issued by the previous administration targeting specific apps and establishes an approach to evaluate connected software applications tied to countries deemed "foreign adversaries," with criteria that include an assessment of ownership, the extent to which an application is subject to coercion, the scope and sensitivity of data collected, and the extent to which any risks can be addressed by independent verification.

**WHAT IT MEANS:** The EO signals the administration's intent to use a case-by-case approach to evaluate China-related risks rather than blanket bans based solely on country of origin. At the same time, the criteria identified as part of the review framework could also serve as a de facto ban based on country of origin, since it is not clear any Chinese-connected software app would be able to pass review without taking mitigation measures such as storing the data in the United States and under the control of a U.S. entity. It also recognizes the possibility that mitigation measures can be used to address risks. These factors are consistent with the stated objectives of the EO (in an accompanying fact sheet): "The Biden Administration is committed to promoting an open, interoperable, reliable and secure Internet." As of February 2024, it appears that the framework has not yet been implemented, at least according to publicly available sources. It is possible that with the new data security EO, the DOJ will take the lead on these issues as focus shifts to that department's new regulatory regime overseeing bulk data transfers to countries of concern.

JANUARY 2021

ICTS Interim Final Rule Issued

- Status: In effect.

**WHAT HAPPENED:** The Commerce Department issues the Interim Final Rule on Securing the Information and Communications Technology and Services (ICTS) Supply Chain, effective March 2021. The rule implements Executive Order 13873 (see below in May 2019) by creating processes and procedures for the Commerce Department to "identify, assess, and address certain transactions, including classes of transactions, between U.S. persons and foreign persons that involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." It describes the ICTS supply chain as underpinning the economy through "the ability to store, process, and transmit vast amounts of data, including sensitive information, that is used for personal, commercial, government, and national security purposes." The rule identifies China as a foreign adversary.

**WHAT IT MEANS:** The broad definitions and scope of the ICTS rule have proved difficult to implement, leading to inaction and debate within the administration regarding the most effective approach.

AUGUST 2020

Trump Administration Seeks to Ban Social Media Apps With Asserted Links to China

- Status: Blocked by courts; revoked and replaced.

**WHAT HAPPENED:** The Trump administration issues two executive orders that, had they been implemented, would have effectively banned these apps in the United States. The orders built upon the May 2019 ICTS EO, identifying the purported risk that U.S. personal information could fall into the hands of the Chinese government.

**WHAT IT MEANS:** The administration shows its willingness to ban products or services on a country-of-origin basis. Both orders ultimately stall in federal courts over freedom of speech and process issues. They are later revoked and replaced by the Biden administration (see above in June 2021).

FEBRUARY 2020

Regulations implement Foreign Investment Risk Review Modernization Act (FIRRMA) overhauls of CFIUS

- Status: In effect.

**WHAT HAPPENED:** The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) had overhauled CFIUS, an interagency group that has the power to block or require modifications in cross-border business deals deemed risks to national security. Treasury Department regulations take effect in February 2020 to implement these changes, including expanding CFIUS' jurisdiction to cover any investments in U.S. businesses that maintain or collect sensitive data. For example, hosting over 1 million individual users' data, maintaining products or services that are used by sensitive U.S. populations, and belonging to certain industries (such as those handling financial, biometric, or geolocation data) can all trigger scrutiny.

**WHAT IT MEANS:** FIRRMA formalized and legitimized CFIUS's longstanding concerns about data access by Beijing. Under its expanded jurisdiction, CFIUS serves as the main mechanism for the U.S. government to address concerns related to protecting sensitive data and national security risks involving aggregation of datasets. As a result, the U.S. approach to data protection relies on a case-by-case review and applies only in circumstances where U.S. businesses receive foreign investment, while not addressing sales of data to third parties around the world. (This changes with the February 2024 EO.) CFIUS also holds the authority to intervene retroactively to review acquisitions involving certain thresholds of user data.

JANUARY 2020

Department of Interior Grounds DJI Drones

**WHAT HAPPENED:** The Department of the Interior (DOI) grounds its drone fleet over data security concerns linked to drones made by the Chinese company DJI and other Chinese-made components. DJI expressed its "extreme disappointment" at the move, which it claimed had "little to do with security" and instead was part of an anti-competitive, "politically motivated agenda."

**WHAT IT MEANS:** Data security concerns are enough to cause the U.S. government to take measures as costly as removing assets it already acquired from service, either losing their utility or requiring replacements. Future procurement decisions are likely to take this kind of risk into account.

MAY 2019

Original ICTS Supply Chain EO Issued

- Status: In effect; build-out continues in interim then final rules.

**WHAT HAPPENED:** The Trump administration issues Executive Order 13873 on "Securing the Information and Communications Technology and Services [ICTS] Supply Chain," granting the Secretary of Commerce authority to prohibit transactions deemed to pose certain security risks in digital technologies that have been "designed, developed, manufactured, or supplied" by companies owned or controlled by "foreign adversaries." (See interim final rule and final rule above.) The term ICTS is defined as "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means."

**WHAT IT MEANS:** This ICTS order does not constitute a blanket ban on such "foreign adversary" technology, but rather sets up a mechanism the U.S. government can use to review, prohibit, or impose mitigation measures if it decides an ICTS transaction is a threat.

# Chinese Policy Developments

SEPTEMBER 2023

Draft Would Relax Outbound Data Transfer Procedures

- Status: Draft, not yet implemented

**WHAT HAPPENED:** The Cyberspace Administration of China (CAC) issues the Provisions on Standardizing and Promoting Cross-Border Data Flows (Draft for Comment). The new rules propose major changes to China's data regime by exempting a wide range of cross-border transfers from pre-transfer administrative approval and/or filing requirements. Examples of such exemptions include transfers of employee personal data, and transfers necessary for activities such as cross-border e-commerce, cross-border payment, air tickets, or hotel booking. Companies may also be exempted from administrative approval and/or filing requirements if they only transfer limited amounts of personal information out of China. Pre-transfer approval would still be required for the transfers of "important data."

**WHAT IT MEANS:** The changes to the cross-border data transfer regime aim to relieve the burden on domestic and foreign companies at a moment of economic headwinds in China. A month before the release of the new draft rules, China's senior leadership signaled its intent to promote private investment and take all necessary measures to boost the economy. With the broad exemptions provided under the new rules, once adopted, the majority of companies' cross-border data flows will be exempted from the requirement to adopt a transfer mechanism. Debate continues regarding the scope of the changes in the draft rules amid competing security and economic objectives for regulating China's digital economy. Moreover, risks around certain kinds of transfers, such as transfers involving "important data," remain under the new regime, including the CAC's ability to investigate or stop certain transfers altogether.

FEBRUARY 2023

Rules Issued Outlining 'Standard Contract' Route for Compliant Data Transfers

- Status: In effect.

**WHAT HAPPENED:** The CAC issues the Measures for the Standard Contract for the Cross-border Transfer of Personal Information, which takes effect in June 2023. For companies that are not required to undertake a security assessment application for their transfer of personal information, this regulation provides that they can adopt a standard contract with a foreign party receiving data. Companies are still required to conduct a personal information impact assessment before transfers and make a filing to the local branch of the CAC, which may accept or reject the filing upon their review.

**WHAT IT MEANS:** Three months after this regulation takes effect, the CAC issues a draft regulation that could exempt most companies from requirements to make a filing for their cross border data transfers. It is therefore unclear how this regulation will be implemented.

SEPTEMBER 2022

Finalized Rules on Outbound Data Transfer Security Assessments

- Status: In effect; revision in draft.

**WHAT IT MEANS:** After several iterations of cross-border data transfer regulations, the final version of the Outbound Data Transfer Security Assessment Measures is finally released and take effect in September 2022. The regulation clarifies the types of cross-border transfers that would be required to pass security assessment, including (1) personal information collected and generated by operators of critical information infrastructure; (2) transfers by companies that have processed personal information of one million or more individuals, (3) transfers by companies that have cumulatively transferred the personal information of 100,000 or more individuals or the sensitive personal information of 10,000 or more individuals. The CAC can also request companies to apply for security assessment in other circumstances when they deem it necessary.

**WHAT IT MEANS:** The regulation shows the government's intention to scrutinize cross-border data transfers by a broad range of companies and by requiring all such companies to undergo a government-led security assessment prior to data transfers. Many companies begin to struggle with the security assessment process, which is time-consuming and burdensome due to the large amount of information requested to be disclosed at the time of submission. One year after the regulation is implemented, the majority of companies who had submitted security assessment applications have not obtained their approval.

NOVEMBER 2021

Personal Information Protection Law Takes Effect

- Status: In effect.

**WHAT HAPPENED:** Serving as China's first comprehensive law in the personal information protection area, the Personal Information Protection Law takes effect on November 1. The law lists obligations imposed on personal information processing entities and empowers individuals with privacy rights. Personal information processing entities that plan to transfer personal information abroad are required to obtain separate notice and consent for the cross-border transfer, on top of general notice and consent for personal information collection. Meanwhile, the entity needs to conduct an internal risk assessment and keep records. Moreover, the entity has to choose one of the lawful transfer mechanisms to transfer personal information overseas.

**WHAT IT MEANS:** The PIPL establishes the framework of China's cross-border personal data transfer regime. That said, the regime is not fully implemented until the issuance of relevant implementing regulations in September 2022, and the detailed requirements on international data flows continue to evolve.

SEPTEMBER 2021

Data Security Law Takes Effect

- Status: In effect.

**WHAT HAPPENED:** China's Data Security Law takes effect on September 1. The law, at a high level, governs data processing activities from a national security perspective and puts an emphasis on the regulation of "important data." It requires, for example, operators of critical infrastructure to localize storage of data or undergo a government-led security assessment justifying the cross-border transfer of data.

**WHAT IT MEANS:** Given that the provisions of the DSL are all high-level, concrete implementation of the law is scant. The concept of "important data," a category that is subject to heightened protection, continues to evolve in various regulations issued by industry regulators, such as the Measures for Data Security Management in the Industrial and Information Technology Sector (Trial) issued by the Ministry of Industry and Information Technology, but so far there is no consistent guidance on how to identify "important data" nor to govern the transfer of such data.

AUGUST 2021

Regulations on Smart Vehicle Data Security

- Status: In effect.

**WHAT HAPPENED:** CAC, together with four other agencies, issues Several Provisions on the Management of Automobile Data Security (Trial). The provisions outline which types of data collected by smart cars are designated as belonging to "important data," which is subject to increased security protections and stricter regulations, including for cross-border data transfer. They also lay out obligations for handling different types of data collected or generated by the vehicle—including about the surrounding environment, drivers and passengers, and infrastructure—which is of use for entities ranging from manufacturers to Internet platforms. Covered entities are required to submit annual reports to the CAC about their data processing activities and data security programs.

**WHAT IT MEANS:** This is the first, and so far the only, regulation offering definitions of "important data" in a particular industry. The definition covers data related to the vehicle itself, but also the infrastructure involved and its surrounding environment, as well as personally identifiable information. Since cross-border transfer of "important data" would be subject to security assessment requirements, transfers of auto data have been subject to much more scrutiny since the regulation took effect.

AUGUST 2021

Critical Information Infrastructure Regulation Issued

- Status: In effect.

**WHAT HAPPENED:** China's new Regulation on Security and Protection of Critical Information Infrastructure stipulates guidelines for operators of critical information infrastructure across a wide range of industries. These guidelines range from implementing a robust cybersecurity program and reporting cybersecurity incidents, to conducting "cybersecurity review" for procurements that could implicate national security. The regulation outlines clear responsibilities for these operators and penalties should they fail to comply with cybersecurity requirements or properly report or evaluate procurements that could affect the security of relevant supply chains.

**WHAT IT MEANS:** The regulation clarifies the scope of operators of critical information infrastructure—a group that other laws and regulations subject to special cross-border data transfer scrutiny—as companies that are treated as critical information infrastructure operators will have to be informed by the regulators. However, there is no public information as to which entities are operators of critical information infrastructure, and no separate data transfer obligations are added here.

JULY 2021

Revised Cybersecurity Review Measures Issued

- Status: In effect.

**WHAT HAPPENED:** An amended version of the Cybersecurity Review Measures, with a draft version issued in July 2021 and the finalized version issued in December 2021, broadens the scope of which procurements of network products and services must be evaluated for national security concerns. Listings on non-Chinese stock exchanges, processing national security-related data, and procuring ICT services and products for use by critical infrastructure operators now warrant a security review by Beijing.

**WHAT IT MEANS:** This revision comes after the first publicized use by the Chinese government of the cybersecurity review regime, targeting ride-hailing firm DiDi after it went forward with an IPO in New York despite reportedly being warned by authorities to delay or desist.

JUNE 2019

Regulation Limits Foreign Access to Genetic Data

- Status: In effect.

**WHAT HAPPENED:** The Regulation on the Management of Human Genetic Resources bars foreigners from collecting human genetic resources or exporting them from China outside the context of a government-approved collaboration. In those collaborations, the Chinese partners must be guaranteed access to all records and data and provided with a backup copy, and they must jointly hold any patent rights. "Genetic resources" here include both physical samples and data or information produced from such samples. These requirements come with increased penalties versus prior interim regulations, and enforcement appears on the rise.

**WHAT IT MEANS:** This regulation forms the basis of the "human genetic resources" (HGR) regime that governs, among other things, data transfers in the clinical trial context, and is vigorously enforced by Chinese regulators to date.

## About the Authors

**SAMM SACKS** is a Senior Fellow at Yale Law School's Paul Tsai China Center, New America's International Security Program, and the Cross Border Data Forum. She is writing a book (to be published by the University of Chicago Press) on the geopolitics of data and U.S.-China relations.

**YAN LUO** is a partner at Covington & Burling LLP. She works with companies to navigate the rapidly evolving regulatory landscape of data in China and other jurisdictions.

**GRAHAM WEBSTER** is a research scholar in the Program on Geopolitics, Technology, and Governance at the Center for International Security and Cooperation, and editor-in-chief of the DigiChina Project, at Stanford University. He researches and teaches about technology and policy U.S.-China relations.

## About DigiChina

The DigiChina Project is a collaborative effort to analyze and understand Chinese technology policy developments through direct engagement with primary sources, providing analysis, context, translation, and expert opinion. It is based at Stanford University, housed within the Program on Geopolitics, Technology, and Governance at the Freeman Spogli Institute for International Studies. More at digichina.stanford.edu.

Stanford | Geopolitics, Technology, and Governance
*Freeman Spogli Institute*