The University of Texas at Austin
Strauss CENTER
for International Security and Law

PROTECTING AMERICANS' PRIVATE INFORMATION FROM HOSTILE FOREIGN POWERS

Prepared Statement of Adam I. Klein

Director, Robert Strauss Center on International Security and Law
University of Texas at Austin

Before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law

September 14, 2022

—

Chairman Coons and Ranking Member Sasse, thank you for inviting me to testify today.

Since the 1990s, American policy has aspired to preserve the ideal of an open, borderless, global internet. Nonetheless, skepticism of cross-border data transfers has spread. Many countries have enacted laws requiring data to be stored locally. Countries invoke shifting rationales—sometimes privacy, sometimes national security—but the result is the same: each year, the internet fragments a bit more.

The borderless internet was a noble aspiration, but it is no longer a viable guide for policymaking. In the People's Republic of China, we now face a formidable peer competitor ruled by a Communist Party (CCP) that holds a fundamentally different vision of politics, global order, and human flourishing. Data flows from the United States can help the CCP achieve that vision and subvert ours.

The U.S. approach to global data flows must reflect these changed circumstances. In this testimony, I will propose four alternative principles to guide our policy on transnational data flows in this era of renewed great-power competition. I will conclude with several recommendations.

1. **Data flows must align with geopolitical realities.**

Recent events remind us that supply chains and trading relationships must be evaluated not merely in economic terms, but against the backdrop of geopolitical dynamics, including the possibility of armed conflict. For example:

- During the COVID-19 pandemic, the United States and many other countries found themselves reliant on China for supplies of Personal Protective Equipment, testing kits, and other vital goods.

- A military fight over Taiwan would remove its dominant share of global semiconductor production from global markets. Congress recently passed the CHIPS Act, which seeks to mitigate this vulnerability by encouraging domestic semiconductor manufacturing.

- Germany's reliance on natural gas imports from Russia has proven to be a costly vulnerability. With pipeline flows now at a standstill, Germany must scramble to conserve gas and secure alternative supplies before the winter.

The last example illustrates the danger of allowing questionable economic links to calcify into strategic vulnerabilities. Despite years of warnings from U.S. officials, including members of this Committee, Germany locked itself into pipeline gas from Russia, failing to invest in new capacity to import liquified natural gas (LNG) from friendly suppliers. Now, Germany finds itself without "a single LNG terminal to receive overseas shipments,"[1] and must rely instead on floating terminals that can handle less than half the gas of Russia's Nord Stream pipeline.

Today's hearing highlights another category of commercial links that create unacceptable security risks: Transfers of U.S. personal data to the People's Republic of China, including transfers facilitated by the growing U.S. market share of certain Chinese technology companies.

The PRC is the only U.S. adversary with the potential ability to fundamentally reshape the global order.[2] Its economic output already equals that of the United States in purchasing power terms.[3] It boasts vast manufacturing output. Technologically, it rivals the United States in certain key sectors—though not yet in others, such as semiconductor design and manufacturing. It is rapidly building a military designed to seize or subdue Taiwan and eject the United States from the Western Pacific. Its leaders see the United States as the main obstacle to China's emergence as the preeminent power in the Pacific and beyond.

Military leaders acknowledge that there is a real chance of military conflict with China this decade. If that occurs, we would have to abruptly unwind our technological entanglements with China—an improvisational scramble that can be avoided by setting sound policies now.

Even if war is avoided, however, such data flows to the PRC weaken the United States in our intelligence, cyber, and technology competition with our most important geopolitical rival.

2. Transfers of Americans' personal data to the People's Republic of China and other hostile foreign powers undermine our national security.

Hostile foreign powers seek U.S. personal data for several purposes, all inimical to our national security.

---

[1] Bojan Pancevski & Benoit Morenne, *Europe Braces for Russia Gas Disruption This Week—and Years of Higher Energy Prices Ahead*, Wall Street Journal, Aug. 30, 2022, at https://www.wsj.com/articles/europe-braces-for-russia-gas-disruption-this-weekand-years-of-higher-energy-prices-ahead-11661858795.

[2] *See generally* Elbridge Colby, *The Strategy of Denial* (2021); Final Report of the National Security Commission on Artificial Intelligence 19 (2021) (hereinafter "NSCAI Report") ("China is a competitor possessing the might, talent, and ambition to challenge America's technological leadership, military superiority, and its broader position in the world.").

[3] *See* https://data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD?locations=US-CN.

Intelligence collection

The PRC and other hostile actors collect U.S. personal data to identify American intelligence officers, target those in possession of defense or industrial secrets for recruitment, and gain access to other sources of information.

Chinese intelligence operations have already harvested vast amounts of U.S. personal data by hacking private companies, such as Marriott, Equifax, and Anthem, and by stealing personnel records from the Office of Personnel Management.[4] We can reasonably assume that those known losses represent only a subset of the overall collection obtained by theft, purchase, and subterfuge.

China can use this data to "to identify existing US intelligence officers through their personnel records and travel patterns as well as to identify potential weaknesses—through background checks, credit scores, and health records—of intelligence targets China may someday hope to recruit."[5] When aggregated and analyzed at scale, it can detect patterns of life that would identify American intelligence officers and their sources. Sensitive personal data—for instance, credit data showing that someone who works for a government agency, defense contractor, or advanced industrial company is deeply in debt—can also be used to target, coerce, or entice Americans of interest to hostile intelligence services. Personal information can also be used to facilitate hacking campaigns that employ spear-phishing or social engineering.

How do we know that transnational data flows containing U.S. personal information would offer considerable intelligence value to the PRC? For two decades, our own intelligence community has leveraged transnational data flows to support counterterrorism and other national-security missions.[6] Surveillance under Section 702 of the Foreign Intelligence Surveillance Act, like precursor efforts that preceded the FISA Amendments Act of 2008, relies on the presence of data pertaining to overseas foreign-intelligence targets on servers and internet backbone cables[7] in the United States.[8] Because the data is on home soil, collection at scale is possible with less operational risk and technical complexity compared to other methods.

---

[4] Department of Justice, *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax* (Feb. 10, 2009) ("For years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax.").

[5] Garrett Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, Wired, Feb. 11, 2020, *at* https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data/.

[6] *See* Office of the Director of National Intelligence, *Section 702 Overview*, *at* https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf ("The government uses the information collected under Section 702 to protect the United States and its allies from hostile foreign adversaries, including terrorists, proliferators, and spies, and to inform cybersecurity efforts.").

[7] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (July 2, 2014), *available at* https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf.

[8] This parallel quickly reaches its limits, of course: Section 702 and technically similar collection by the PRC serve utterly different ends, in terms of the legitimacy of the constitutional orders they serve and how the collection can be

Section 702 illustrates the considerable intelligence value that can be derived from inbound data flows. We should be pleased that *our own* intelligence agencies can use these tools to uncover foreign threats. Our allies also derive considerable benefit from Section 702.[9]

Conversely, we should use every reasonable measure to prevent the PRC from obtaining the same advantage. Inbound data flows enhance the ability of PRC intelligence services to repress dissidents and minorities at home, harass dissidents abroad, threaten Taiwan and other U.S. partners and allies, steal American intellectual property, and prepare for war against the United States.

How to prevent China from duplicating this success? Recall that Section 702's home-field advantage is a byproduct of our centrality in the global internet economy. Data travels to and through the United States because we were the first mover, and remain the leader, in new internet technologies.

It follows that the global expansion of Chinese internet companies should be seen not merely as a commercial challenge, but also as an intelligence threat. This has been widely recognized, and ably countered in some instances, in the case of Chinese *hardware*.[10] We should regard flows of sensitive personal data the same way. Below, I discuss how to apply this principle to outflows of U.S. personal data to the PRC.

Transnational repression

In recent years, the Justice Department has repeatedly indicted agents of authoritarian foreign powers for harassing or threatening peaceful regime opponents who have sought refuge in the United States. For example, in July, DOJ charged five defendants with clandestinely plotting to harass, discredit, and surveil PRC critics living in the United States.[11] Access to U.S. data facilitates these efforts. According to a *New York Times* report, PRC security officials and contractors use "advanced investigation software, public records and databases to find [the] personal information and international social media presence" of regime critics, including "those living beyond China's borders."[12]

Lax controls on the sale of Americans' personal data facilitate this repression. While "U.S. regulators have repeatedly blocked Chinese deals to acquire American technology

---

used. Section 702 may be used only for purposes approved by life-tenured federal judges and is overseen by Congress and other independent bodies. Such constraints are unknown in the PRC's Party-state.

[9] *See* Adam I. Klein, Chairman, U.S. Privacy and Civil Liberties Oversight Board, *Statement on the Terrorist Finance Tracking Program*, at 1 n.2 (Nov. 19, 2020) (citing examples), *available at* https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.

[10] *See, e.g.*, Rory Cellan-Jones, *US cyber-boss tells UK to 'think again' on Huawei*, BBC, Feb. 21, 2020, *at* https://www.bbc.com/news/technology-51581095.

[11] *See* DOJ Office of Public Affairs, *Five Men Indicted for Crimes Related to Transnational Repression Scheme to Silence Critics of the People's Republic of China Residing in the United States* (July 7, 2022), *at* https://www.justice.gov/opa/pr/five-men-indicted-crimes-related-transnational-repression-scheme-silence-critics-people-s.

[12] Muyi Xiao and Paul Mozur, *A Digital Manhunt: How Chinese Police Track Critics on Twitter and Facebook*, New York Times, Jan. 1, 2022, *available at* https://www.nytimes.com/2021/12/31/technology/china-internet-police-twitter.html.

companies over the access they provide to personal data," the story notes, our government has thus far done relatively little to "control the widespread availability of online services that offer location data, social media records and personal information."[13]

Training AI models

Machine learning requires large amounts of high-quality training data. The resulting algorithms are typically most accurate when applied in real-world settings that resemble the training data.

Why does China need American data to build AI? It is often said that the vast amount of data available in China, with its immense population, gives it an advantage in the race to develop sophisticated AI. If that data pertains primarily to Chinese citizens, however, it may not be predictive of behavior, events, or trends in the United States, a far more diverse society with different modes of social and political organization.

3. The United States must restrict sensitive data flows to the PRC and other major adversaries.

In most sectors of the economy, U.S. law and policy have presumed that data should flow freely across borders to where it is most efficient for the provider and most convenient for the user. That aligns with the general American approach of allowing innovation to proceed, absent an express prohibition. European regulators, by contrast, tend to employ the "precautionary principle," under which regulators must first approve a new business method or product before economic actors can move forward.[14]

That data should move freely across national borders is not the majority position among advanced economies. The European Union, in particular, has long embraced a different principle: that personal data can only be transferred to countries that offer an "adequate level of protection," with adequacy determined by the European Commission in the first instance and ultimately by the Court of Justice of the European Union.[15] Ironically, that principle has been applied most aggressively to Europe's most important ally, the United States, in a series of decisions by the Court of Justice of the European Union.[16]

In general, American law's comfort with cross-border data flows remains a net positive. It has contributed to the United States' emergence as the unquestioned, and until recently unchallenged, leader in the development of the global internet. American companies have become globally dominant in many fields, including cloud computing, which requires that data be dispersed to ensure secure and efficient service.

Openness ceases to be a virtue, however, when data moves to the small group of countries determined to do us ill. Capable intelligence services can extract great intelligence

---

[13] *Id.*

[14] *See, e.g.*, Treaty on European Union (Maastricht Treaty), art. 130r (1992) ("Community policy on the environment shall … be based on the precautionary principle…").

[15] *See* EU Directive 95/46, art. 25; General Data Protection Regulation, arts. 44-45.

[16] *Schrems v. Data Protection Commissioner*, C-362/14, ¶¶ 2, 27 (C.J.E.U. Oct. 6, 2015); *Data Protection Commissioner v. Facebook Ireland Ltd.*, C-311/18, (C.J.E.U. July 16, 2020) (*Schrems II*).

value from flows of data that do not overtly relate to national security. It is telling that China operates on this assumption too: Last year, for example, the Chinese Communist Party banned cars made by Tesla Motors from the Baidohe beach resort, the prestigious seaside retreat for senior CCP officials. The reason: fears that the cars could record video and other information of potential intelligence value to the United States.[17]

With the PRC emerging as a peer competitor that seriously threatens major war, we can no longer afford to trade economic benefits for security vulnerabilities. In the 1990s and 2000s, it was widely believed that economic engagement with China would moderate the CCP and ultimately transform China's system of government. That is now recognized as a fallacy.[18] Economic engagement has enriched and strengthened the CCP, even as it has become implacably hostile to the United States and our presence in the Western Pacific. We must revise our economic arrangements with China, including data flows, to reduce the strategic advantages the PRC derives from them.

4. The presumption of openness should be revised to embrace free flows of data *among friendly nations*.

What principle should replace the presumption that most data should flow freely across borders?

The United States should not embrace the European Union's approach, which holds that the "adequacy" of a country's data-governance regime, measured against abstract privacy-related principles, should determine whether data can flow. Innovation and commerce have benefited from a general presumption that data can move as the needs of businesses and users dictate. That light touch should be preserved.[19]

Instead, the United States should adopt and seek to advance internationally the principle that data should move freely *among friendly nations*, broadly defined to include countries that maintain amicable relations with the United States and whose strategic interests are not fundamentally opposed to ours. Among those countries, data should move freely unless it falls within certain highly sensitive categories.

This approach would align with proposals by important U.S. allies. Most notably, Japan's "Osaka Track" initiative, described by the late Shinzo Abe as embodying "Data Free Flow With Trust," envisions open data flows as the default, but acknowledges that some nations

---

[17] Eamon Barrett, *China is banning Tesla owners from driving near the government's summer retreat, another sign Beijing considers the vehicles U.S. spies*, Fortune, June 21, 2022, *at* https://fortune.com/2022/06/21/china-ban-tesla-beidaihe-government-retreat-data-security-spy/.

[18] *See* Kurt M. Campbell and Eli Ratner, *The China Reckoning: How Beijing Defied American Expectations*, Foreign Affairs (March/April 2018) ("Neither carrots nor sticks have swayed China as predicted. Diplomatic and commercial engagement have not brought political and economic openness. Neither U.S. military power nor regional balancing has stopped Beijing from seeking to displace core components of the U.S.-led system. And the liberal international order has failed to lure or bind China as powerfully as expected. China has instead pursued its own course, belying a range of American expectations in the process."), *available at* https://www.foreignaffairs.com/articles/china/2018-02-13/china-reckoning.

[19] Reciprocal restrictions or other trade remedies may be necessary, however, if other countries restrict data transfers to the United States.

may opt to restrict the movement of certain categories of data, to certain countries, based on security imperatives.[20] The APEC Cross-Border Privacy Rules, which embrace many U.S. allies and partners in the Pacific, similarly reflect a desire to "avoid barriers to information flows" while recognizing the need for some limitations based on national security.[21]

Note that this principle would leave unimpeded data transfers to many countries that, while U.S. allies or partners, are reputed to conduct intelligence collection against the United States. This contrasts with European law, as interpreted by the Court of Justice of the European Union, which has repeatedly struck down determinations that the United States provides "adequate" protection.[22] In both cases, the court's decision turned on the possibility that U.S. intelligence agencies could access data transferred across the Atlantic.

The United States should reject and resist the European Union's universal "adequacy" requirement, for at least two reasons.

First, if adopted by other nations and applied consistently, the European approach would bring global data transfers to a halt.[23] Few nations have spotless hands in the murky world of intelligence. Media reports suggest that European governments target Americans for intelligence collection, including for the commercial advantage of local companies—something the United States forswears as a matter of policy.[24] If the European Union's "adequacy" principle, as interpreted by the Court of Justice of the EU, were applied reciprocally, companies such as Airbus, BMW, and Siemens would be barred from sending customer data from the United States to Europe, because of the possibility that it would be intercepted by European intelligence services. This is not a constructive path for allies to follow.

Second, it makes little sense to obstruct data flows based on the possibility of intelligence collection without regard to the geostrategic alignment of the countries involved. Data flows to China provide an intelligence advantage to a strategic adversary, undermining the security of the United States and Europe. American intelligence collection, by contrast, *strengthens* European security: Section 702, the Terrorist Finance Tracking Program, and other U.S. intelligence

---

[20] *See* World Economic Forum White Paper, *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*, at 14 (May 2020) ("While some jurisdictions are open and make no distinction between foreign or domestic entities in their data protection rules, most jurisdictions make a distinction between domestic and foreign entities for data that is perceived to pertain to national security, or they designate specific entities as either trusted or of particular high risk – where some jurisdictions also routinely categorize all data as being sensitive.").

[21] *See* APEC Privacy Framework, preamble and art. 18. The United States, Mexico, Japan, Canada, Korea, Singapore, Australia, the Philippines, and Taiwan currently participate in the APEC Cross-Border Privacy Rules System; the PRC does not. *See* http://cbprs.org/documents/.

[22] *See supra* n.16 (citing *Schrems I* and *II*).

[23] The principle is not applied consistently. A 2015 European Commission report on data transfers to China candidly acknowledged that "[i]f a legalistic approach [were] adopted, … *data transfers would need to be prohibited towards China* on the basis of Article 25 of the EU 1995 Data Protection Directive," the provision at issue in Schrems, and whose operative principle is now enshrined in the GDPR. Directorate-General for Internal Policies, *Report for the European Parliament LIBE Committee: The Data Protection Regime in China*, at 28 (2015) (emphasis added).

[24] *See* Adam Rawnsley, *Espionage? Moi?*, Foreign Policy, July 2, 2013, *at* https://foreignpolicy.com/2013/07/02/espionage-moi/; Deutsche Welle, *Hillary Clinton's phone 'hacked by German intelligence'*, Aug. 15, 2014, *at* https://www.dw.com/en/hillary-clintons-phone-hacked-by-german-intelligence/a-17857728.

activities provide a consistent flow of counterterrorism intelligence to European partners.[25] More fundamentally, the U.S. military forms the backbone of NATO, through which the United States is committed to the conventional and nuclear defense of European allies. Effective intelligence collection is integral to that defense, as the conflict in Ukraine amply demonstrates.

Any principle that is agnostic as between an ally that has pledged its strength to one's defense and a totalitarian strategic adversary is deeply flawed.

5. Recommendations

In this section, I offer several recommendations to implement these principles and reduce the vulnerabilities created by data transfers to hostile powers.

A. Congress should prohibit transfers of sensitive personal data concerning Americans to a set of enumerated hostile foreign powers.

The prohibition should include, at a minimum, the PRC (by far the most significant destination for transfers of concern) and the Russian Federation. It should apply to American companies and foreign companies operating on U.S. territory or whose user base in the United States exceeds a certain threshold. The law could include a designation mechanism permitting the Secretary of Commerce to add additional foreign powers, though the PRC and Russian Federation should be covered by statute.

Covered data should be defined broadly enough to encompass the most sensitive categories of information that are frequently collected: biometric information or identifiers, personal health information, genetic data, location-tracking data, financial or credit information. It should also include a catch-all embracing other information that bears upon the intimate private affairs of the subject.[26]

Congress may also wish to consider applying the law extraterritorially in certain circumstances. For example, the law could contain a criminal prohibition on knowingly facilitating surreptitious transfers of covered data to a hostile foreign power.

---

[25] *See* Adam I. Klein, Chairman, U.S. Privacy and Civil Liberties Oversight Board, *Statement on the Terrorist Finance Tracking Program*, at 1-3 & n.2 (Nov. 19, 2020), available at https://documents.pclob.gov/prod/Documents/EventsAndPress/b8ce341a-71d5-4cdd-a101-219454bfa459/TFTP%20Chairman%20Statement%2011_19_20.pdf.

[26] Such a catch-all category is necessary but difficult to define with precision. German law is illustrative: it bars surveillance that touches upon the "innermost sphere of private life" (*Kernbereich privater Lebensgestaltung*). *See* Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10), § 5a (Schutz des Kernbereichs privater Lebensgestaltung). A recent decision by Germany's Federal Constitutional Court elaborates that "development of one's personality in this innermost sphere of private life includes the possibility of expressing one's internal processes, sensations, feelings, thoughts, opinions, and experiences of a most personal character," in particular through "non-public communications" with trusted third parties, which the person reasonably expects will not be surveilled. The principle also applies with special force in private living spaces. Urteil zum Bayerischen Verfassungsschutzgesetz, 1 BvR 1619/17, ¶¶ 275-286 (Bundesverfassungsgericht, Apr. 26, 2022), *available at* https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2022/04/rs20220426_1bvr161917.pdf?__blob=publicationFile&v=3.

B. At a minimum, Congress and the Executive Branch should sharply curtail business practices of Chinese companies that could enable CCP authorities to access sensitive U.S. data at scale.

The risks presented by Chinese applications, most notably TikTok, have been widely documented.[27] The copious data collected by these apps is potentially accessible to employees of these companies in China, where the law requires companies to assist the government in national-security matters and submit to opaque data audits.

These companies insist that corporate policies ensure that data will remain in the United States, or that they would resist demands for access by the Chinese government. But internal policies are permeable, and even technical barriers written into code are only as secure as the next software update. Ultimately, the realities of power in a "Party-state," where government organs are subordinate to the Communist Party, make it naïve to assume that any supposed constraints would impede the CCP when it perceives a threat to its internal or external security interests. The precise nature of access permitted by Chinese statutes and regulations is a distraction: We must assume that any type of data, access, or control that is technically possible and that the CCP believes to be in its interest will be demanded and provided.

There have been some successes. In 2019, the Committee on Foreign Investment in the United States forced Chinese company Kunlun Gaming to divest dating app Grindr.[28] Thus far, however, the U.S. government not taken decisive action to curb the penetration of Chinese apps in the U.S. market. TikTok continues to expand, despite reports that "China-based employees of [TikTok parent company] ByteDance have repeatedly accessed nonpublic data about US TikTok users."[29]

The data that TikTok collects from each user would be valuable to any intelligence agency. As FCC Commissioner Brendan Carr has explained:

> TikTok functions as a sophisticated surveillance tool that harvests extensive amounts of personal and sensitive data. Indeed, TikTok's own disclosures state that it collects everything from search and browsing histories to keystroke patterns and biometric identifiers, including faceprints—which researchers have said might be used in unrelated facial recognition technology—and voiceprints. It collects location data as well as draft messages and metadata, plus it has collected the text, images, and videos that are stored on a device's clipboard. The list of personal and sensitive data it collects goes on from there.[30]

---

[27] *See, e.g.*, Letter from FCC Commissioner Brendan Carr to Tim Cook and Sundar Pichai (June 24, 2022), *at* https://www.fcc.gov/sites/default/files/carr-letter-apple-and-google.pdf.

[28] *See* Yuan Yuan and James Fontanella-Khan, *Grindr sold by Chinese owner after US national security concerns*, Financial Times, Mar. 7, 2020.

[29] Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, Buzzfeed News, June 17, 2022.

[30] Testimony of Brendan Carr, Commissioner, Federal Communications Commission, before the Subcommittee on National Security of the House Committee on Oversight and Reform, *Protecting Military Servicemembers and Veterans from Financial Scams and Fraud* (July 13, 2022).

TikTok's success with young Americans also raises concerns that its algorithm could be manipulated to influence public opinion during a U.S.-China crisis. For example, the algorithm could be tweaked to promote popular videos critical of American policy or deepfake videos intended to spread panic and division among Americans. These scenarios may seem farfetched, but it is only prudent to plan around what is technically possible given the design and market-penetration of the app.

Payments are another vulnerability. Chinese payment app Alipay is increasingly accepted by U.S. merchants, including CVS. Payment apps produce a stream of financial data that would have considerable value for PRC intelligence services. At present, Alipay users outside China appear to be primarily Chinese citizens traveling abroad.[31] By accepting Alipay and other PRC payment apps even under these limited circumstances, however, U.S. retailers are helping lay the groundwork for PRC-based payments networks that reach more broadly into the United States and allied countries.

Internet of Things devices are another potential source of data-leakage to the PRC. As the researcher Aynne Kokas has noted, many Chinese-built Internet of Things devices transfer the data they collect to servers in China. These products may record intimate details about what takes place in the home, on corporate networks, and in other sensitive locations. If these devices are used by Americans of interest to the CCP, the data they produce can be accessed by PRC intelligence services for compromise, extortion, social engineering, and other malign actions.

Hostile foreign powers are aware of the potential vulnerability that emanates from such data. Several years ago, Russia passed legislation requiring foreign companies to store Russian users' data on in-country servers. China demanded that Apple do the same with local iCloud backups[32] and has kept other prominent American internet firms out altogether. What they fear of us, we should expect them to do *to* us, if given the chance.

Recent reports that the Administration will soon issue an Executive Order to curtail data leakage to the PRC are welcome.[33] It will ultimately fall to Congress, however, to create a comprehensive, enduring statutory regime to reduce data leakage to hostile foreign powers.

---

[31] *See* Kate Silver, *The new wave of global trade: How Alipay connects US businesses with Chinese consumers* (paid content sponsored by Ant Group] ("It's a Chinese app for Chinese consumers. They can use it for online as well as in-person transactions in China, and also when they travel abroad, including in the United States. And so American businesses can accept it as a method of payment for both online and in-person transactions in China and the United States to transact with Chinese consumers who are traveling here."), *available at* https://www.protocol.com/sponsored-content/the-new-wave-of-global-trade-how-alipay-connects-us-businesses-with-chinese-consumers?rebelltitem=2#rebelltitem2.

[32] *See* Aynne Kokas, *Cloud Control: China's 2017 Cybersecurity Law and its Role in US Data Standardization*, at 9 (2019) ("[F]or Apple, as for many other companies in areas ranging from engineering services to enterprise computing, the decision to open a data center with major ownership by a Chinese firm transforms the politics of power and access to data within the company and among its consumers."), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427372.

[33] *See* Reed Albergotti, *Biden will crack down on Chinese tech with a new executive order*, Semafor, Sept. 2, 2022, *at* https://medium.com/semafor-media/semafor-exclusive-biden-will-crack-down-on-chinese-tech-with-a-new-executive-order-da466c263a8a.

C. Congress must better regulate data brokers, whose present business model all but guarantees that sensitive data about Americans will pass at scale to hostile foreign powers.

Data brokers purchase data from apps, ad-tech companies, websites, and other parts of the internet economy. They then aggregate that data and sell it to third parties. This data can be highly sensitive, including such information as browsing history, purchasing details, consumer profiles, intimate details about personal characteristics revealed through online habits and app use, and location.[34]

As long as this business model persists, it will remain virtually impossible to prevent this information—and the intelligence bounty that it represents—from falling into the hands of hostile foreign powers. Even if data brokers were be prohibited from knowingly selling to foreign powers or their representatives, foreign intelligence services could use subterfuge to evade these controls. Brokers have little ability or incentive to conduct robust diligence. The national-security rewards of curtailing this business model would be among the benefits of passing comprehensive data-privacy legislation during this Congress.

Thank you for the opportunity to testify today. I look forward to your questions.

* * *

[34] *See* Justin Sherman, *The Open Data Market and Risks to National Security*, Lawfare, Feb. 3, 2022 ("Foreign citizens, companies and governments can legally buy highly sensitive data on Americans from U.S. companies."), *at* https://www.lawfareblog.com/open-data-market-and-risks-national-security.