Corporate Complicity: Subsidizing the PRC's Human Rights Violations

Testimony of Dr. Aynne Kokas
C.K. Yen Chair, Miller Center for Public Affairs
Director, University of Virginia East Asia Center
Non-Resident China Studies Fellow, Baker Institute for Public Policy, Rice University
Associate Professor of Media Studies, University of Virginia
Congressional-Executive Commission on China
July 11, 2023

Chairman Smith, Cochairman Merkley, and distinguished members of the Congressional-Executive Commission on China, it is an honor to present my testimony.

As the United States (U.S.) grapples with how to approach China's expanding digital influence, it is imperative to explore the role of U.S. corporations operating in the country as well as firms that serve as U.S.-based data brokers. My testimony explores the ways that fragmented U.S. data oversight laws interact with Chinese government data oversight to pressure corporations to prioritize compliance with Chinese laws and policies. Additionally, I delve into similar dynamics that have fueled misinformation and censorship in the media sector. Drawing from my recent books, *Trafficking Data: How China is Winning the Battle for Digital Sovereignty* (2022) and *Hollywood Made in China* (2017), I make recommendations to reduce U.S. corporate digital rights violations by Chinese firms, as well as firms operating as data brokers in the U.S. I argue for the importance of focusing attention on how to bring overarching US digital oversight into line with our allies and partners to better serve as a countervailing force against pressure companies face from Chinese government regulations. I look forward to the discussion and would be happy to expand on any of these points during questioning.

My testimony focuses on four key findings:

1. U.S. data oversight laws follow a risk-based model, which assumes corporations have the capacity to mitigate harm.
2. Many Chinese corporate data oversight laws have expansive extra-territorial scope and lack transparency. The opacity of these laws makes it difficult to determine the extent to which firms are exploiting data in the normal course of their operations
3. Without comprehensive data protections in the U.S. and the potential for financial, civil, and criminal penalties in China, companies must navigate a complex legal landscape.
4. The intersection of pressures for Chinese market access with weak U.S. laws have further created an environment ripe for censorship and disinformation.

U.S. technology oversight assumes the capacity to mitigate harm. However, there are currently no comprehensive data security laws in place either domestically and extra-territorially.

Fragmented sector-based and state-based oversight fails to keep pace with evolving technologies, leaving U.S. citizens vulnerable to data breaches and exploitation.

Sector-based oversight, such as the Health Insurance Portability and Accountability Act (HIPAA), neglects key areas of the health technology sector, from commercial DNA testing to medical devices to smart watches. The Children's Online Privacy Protection Act (COPPA) requires parental consent for self-disclosure of information by children under 13,[1] but has serious limitations—it protects children under 13 only when information is shared by them, rather than by an adult.[2] Once a parent consents to the child's self-disclosure, sites can freely collect any shared information.[3] Moreover, the law does not appear to cover household-level (rather than individual-level) data that might include that of children under 13, such as that collected by Google Home and Amazon Alexa devices.[4]
By failing to update existing sector-based laws to reflect the breadth of opportunities for data-gathering by firms, it becomes impossible to move forward with even the most basic standards of user data protection.

State-based oversight further fragments the U.S. corporate data security landscape, with state legislatures facing pressure to oversee complex laws that often exceed their technical capacity, budgetary constraints, and scope of oversight. While states with more technical resources already offer digital rights enforcement to their citizens (e.g. enhanced protections of biometric data for Illinois residents, financial data for New Yorkers, and user data for those living in California, Utah, and Virginia) create a patchwork of data protection regulations across the country. For example, there are multiple competing standards for how people in different states can use popular apps like TikTok and WeChat. This makes it difficult for U.S. businesses and citizens to navigate the complex and often conflicting regulatory environment.

Adding to this complexity are third-party data brokers, who acquire and sell corporate data. In bankruptcy proceedings, banks can require firms to liquidate their data as an asset, increasing the vulnerability of user data.[5] Data broker activity in bankruptcy proceedings and elsewhere further fragments U.S. data oversight and highlights the need for comprehensive national data protection regulations.

---

[1] Federal Trade Commission. "Children's Online Privacy Protection Rule ('COPPA')."
[2] Federal Trade Commission. "Children's Online Privacy Protection Rule ('COPPA')."
[3] Federal Trade Commission. "Children's Online Privacy Protection Rule ('COPPA')."
[4] Smith, "Voice-Captured Personal Data."; Haber, "Internet of Children."; Lutz and Newlands, "Smart Speakers."
[5] Guillou, "Privacy Issues in Bankruptcy Sales."

Corporate and user data form the foundation of a wide range of emerging information and communication technologies. It is important to prevent data trafficking, the uncontrolled movement of commercial data across borders through government pressure, not just for immediate security purposes, but also to protect long-term competitiveness in communications, artificial intelligence, healthcare, payments, and other critical sectors.

Chinese laws, by contrast, are wide-reaching with strong data localization requirements, unclear enforcement or statutes of limitation, and an extraterritorial scope.

The Cybersecurity Law of the People's Republic of China[6, 7] requires critical information infrastructure data to be stored in China. China's Personal Information Protection Law (PIPL) offers enhanced data localization requirements beyond the critical information infrastructure data localization which makes transfer of data overseas subject to a security assessment by the Cyberspace Administration of China.[8] Article 3 of PIPL includes broad corporations that process personal information within China's borders, emphasizing the extraterritorial nature of the law's scope.

PIPL is one of many Chinese that laws that implicate the worldwide corporate operations. The "Provisions on the Governance of the Online Information Content Ecosystem" asserts potential criminal or civil liability for consuming, producing or sharing "negative" information. The Law of the People's Republic of China on Safeguarding the National Security in the Hong Kong Special Administrative Region, colloquially known as the Hong Kong National Security Law, permits the Chinese government to hold people and platforms liable for crimes committed extraterritorially, which puts particular pressure on firms with large Chinese operations[9].

Further, most Chinese digital oversight laws lack clear enforcement parameters, encouraging corporations to comply with the most conservative interpretations of the law. The Provisions in Online Governance, Cybersecurity Law, Personal Information Protection Law and Hong Kong National Security Law all lack clear enforcement provisions, but one of the more interesting opportunities for government access to corporate data is China's national security audit system, established by the 2021 Data Security Law[10], that can review any activities that influence or might influence national security data. All companies operating in China are subject to the regulations, and the scope of what constitutes national security data is neither fixed nor

---

[6] Standing Committee of the National People's Congress, 中华人民共和国网络安全法 [Cybersecurity law of the People's Republic of China].

[7] Creemers, Triolo, and Webster, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)."

[8] Julia Zhu, "The Personal Information Protection Law: China's Version of the GDPR?," Columbia Journal of Transnational Law.

[9] The National People's Congress, 中华人民共和国香港特别行政区维护国家安全法 [Law of the Hong Kong Special Administrative Region of the People's Republic of China on Safeguarding State Security]

[10] Rafaelof et al, "China's 'Data Security Law (Draft)'."

transparent. Through the data audit process, regulators can pressure firms to share data with the Chinese government as a condition of their continued operations.

Corporations gathering user data in the United States that are subject to Chinese laws face significant pressure to comply with Chinese laws in the absence of comprehensive U.S. data protections.

This dynamic is apparent in the Internet of Things (IoT). Haier, a Chinese company, purchased GE Appliances in 2016 for $5.4 billion,[11] the world's largest consumer appliance company.[12] Since then, Haier has launched an entire line of connected consumer electronics called GE Smart Appliances[13] that gather data and store it on apps developed by Haier U.S. Appliance Solutions, Inc. Haier has also developed the U+ Connect platform, which collects data through all connected GE Appliances and Haier-connected products.[14] Haier uses Baidu's TianGong smart IoT platform to connect equipment, manage devices, and store data for the U+ Connect platform that GE Appliances use,[15] thereby integrating GE Appliances into China's data storage system.

Precision agriculture is another prominent area where this dynamic plays out. Syngenta, a firm that gathers and integrates data about agricultural yields,[16] is one of precision agriculture's major players. ChemChina, the state-owned China National Chemical Corporation, became the world's largest supplier of pesticides and agrochemicals with its $43 billion acquisition of Syngenta in 2017 and it is also the top pesticide seller in North America.[17]

Syngenta collects data via drones and satellites to help farmers manage crop yields[18] and sells seeds, fertilizers, and pest management to AgriEdge users at a discount. AgriEdge has become integrated into the U.S. agricultural landscape, covering 10.5 million acres of arable U.S. land in 2021, with more than 95% of growers using whole farm management systems from Syngenta.[19]. Even the Ram, a popular farm vehicle which holds a greater than 25% stake in the U.S. truck market, now offers packages that include AgriEdge.

By integrating the U.S. agricultural and IoT ecosystems with a firm owned by a Chinese state-owned enterprise, the U.S. is taking a risk that the extraterritorial nature of Chinese laws will force firms to share key data about how U.S. homes and agricultural ecosystem's function. I discuss other examples in the gaming, social media, satellite, smart city, and payment sectors in

[11] Yu, "Haier Has A Plan."
[12] GE Appliances, "Time-Saving Technologies."
[13] GE Appliances, "Time-Saving Technologies."
[14] GE Appliances, "Time-Saving Technologies."
[15] Tencent Tech, "Baidu, Haier Partner."
[16] Syngenta Global, "Our Research Areas."
[17] M&A Critique, "ChemChina Buys Out Syngenta."
[18] Tully, "Drones to Modernize Farming."; McMahon, "Drones Provide a Bird's Eye View."; Ostrom, "New Pilot Program Delivers Innovative Digital Technology."
[19] Syngenta US, "AgriEdge."

my book, *Trafficking Data*. However, regardless of the sector, the Chinese firms face no legal data storage requirements in the United States.

Beyond industry-specific exposure, COVID-19 protocols in China control the behavior of people working at corporations in China. Access to essential payment, mobility, and communication apps in China now require sharing, at a minimum, one's passport number or residence card number, but more commonly, a Chinese bank account, enabling both monitoring and punitive action. Such technical systems require individuals doing anything in China, whether visiting family, working, or doing research, to either depend on a Chinese colleague or friend, allow tracking, or submit oneself for the scrutiny of a residence permit, to engage in the most basic activities of living. When using a term like corporate complicity, it is important to recognize that many of the workers or corporations in question must balance their ability to continue to function.

Pressures for Chinese market access interact with weak U.S. laws to contribute to censorship and disinformation.

These shifts in market power are changing our digital landscape in two key ways.

First, firms are changing the content they produce. To gain access to China's profitable but tightly regulated media market, Hollywood studios must comply with Chinese censorship rules, which can impact the content of films. For example, in "Doctor Strange," the character of The Ancient One was portrayed as a Tibetan monk in the original version of the movie, but in the Chinese version, this character was changed to be a Celtic woman to avoid offending the Chinese government, which does not recognize Tibet as an independent country.[20] Similarly, the villainous character of The Mandarin, who is portrayed as a villain in the original version of the movie, was changed to be a non-Chinese character in the Chinese version.[21] While it is clear that yellow peril stereotypes like those visible in characters like The Ancient One and The Mandarin present problematic representations of race, it is the market under which studios changed those characters that is most significant. In *Mulan* (2020), the film's global release evoked Chinese central government narratives urging the prioritization of the central government at the expense of dangerous borderlands.[22]

[20] Child, "Tilda Swinton Cast."
[21] Zakarin, "Chinese Cut of 'Iron Man 3.'"
[22] Kokas, "Hollywood needs China."

Figure 1: Nine-dash line maritime claim in *Abominable* (2019)

Source: *South China Morning Post*

Second, firms are extending Chinese market policies globally in the absence of laws. The University of Toronto's Citizen Lab reported that accounts that fall under WeChat's Chinese terms of service, accounts first registered in China or "China-registered-accounts," are subject to "pervasive political censorship" even outside of China, even when those accounts move to international numbers.[23] This includes foreign students, immigrants, and businesspeople who first download WeChat in China, but switch phone numbers when they move outside of China.

Recommendations

The following recommendations are based on my award-winning books *Trafficking Data: How China is Winning the Battle for Digital* Sovereignty (Oxford University Press, 2023) and *Hollywood Made in China* (University of California Press, 2017). These strategies are critical for reducing U.S. corporate violations of digital rights violations in relation to Chinese firms, and all firms that serve as data brokers in the United States.

- **Work with Allies and Partners to Establish Standards for Data Transfer**
    - Review and align the US with adequacy standards for cross-border data transfer established by the European Union and Japan.
    - Join key trade agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CP-TPP) and other trade agreements that enhance

[23] Knockel et al, "We Chat, They Watch."

transparency in cross-border data transfers while also requiring the protection of personal information for users.

- **Enhance U.S. Oversight to Prevent International Data Trafficking**
    - Work with states to harmonize state-level data security oversight through federal legislation. This could include practices such as issuing best practices for state data-security oversight. Grants for specific state-level data security projects would help to enhance state-level technical oversight capacity.
    - Build out a national data privacy framework to prevent consumer data exfiltration to non-allied countries. Such a move is important not just to protect user data, but it is also essential to help build consensus among democratic allies, many of whom have different approaches to data oversight than the United States.
    - Enhance technology sector collaboration across developed democracies as outlined in the S. 604 Democracy Technology Partnership Act.
    - Develop more precautionary approaches to the use and introduction of ICT products and services. Approaches like the bipartisan S.686 RESTRICT act represent an important first step.
    - Regulate the data broker industry in the U.S. S.631 UPHOLD Privacy Act of 2023, S.1029 Protecting Military Servicemembers' Data Act of 2023, and H.R. 3045 You Own the Data Act and others offer first steps in this direction.
    - Enhanced SEC reporting of data storage practices by publicly-traded firms would use existing reporting mechanisms to enhance corporate accountability for how, when, and where firms share their data. Explore ways to require data storage and security reporting by privately-held US firms. Improved transparency in data storage and security practices is valuable not just in its ability to track data trafficking, but also provides helpful metrics to include data storage and security in environmental, social, and corporate governance investment indices.

Fund Chinese area studies so that workers can better understand the implications of their business decisions related to China. The lack of secondary and tertiary education opportunities to learn about China means that most people entering the U.S. workforce do not have a working understanding of China's political system which can lead to uninformed decision-making both in terms of the under- and over-estimation of risk. Funding from Title VI, the Fulbright US student China program, the East-West Center, the Woodrow Wilson Center, the National Endowment for the Humanities, and the Kluge Center at the Library of Congress, has been central to my ability to research and teach about China at the University of Virginia and as a student in public universities in California and Michigan. To prevent corporations from enabling human rights violations, there is a crucial national security need to fully fund the study of China and Chinese by American students and scholars.

Bibliography

Baldwin, Clare, and Kristina Cooke. 2015. "Special Report: How Sony sanitized Adam Sandler movie to please Chinese censors." *Reuters*, July 24, 2015. Accessed March 10, 2020. https://www.reuters.com/article/us-china-film-specialreport-idUSKCN0PY1OJ20150724.

Business of Technology. 2021. "2021 IT (Information Technology) Industry Trends Analysis." Last Modified 2021. http://connect.comptia.org/content/research/it-industry-trends-analysis https://connect.comptia.org/content/research/it-industry-trends-analysis.

Chen, Ming Shin. 2019. "China's Data Collection on U.S. Citizens: Implications, Risks, and Solutions." 15 (1):14.

Child, Ben. "Tilda Swinton Cast as Tibetan to Placate China, Says Doctor Strange Writer." The Guardian, April 26, 2016. https://www.theguardian.com/film/2016/apr/26/doctor-strange-tilda-swinton-whitewashed-china.

China Law Translate. 2019. "网络信息内容生态治理规定 – Governance of the Online Information Content Ecosystem." *China Law Translate*. https://www.chinalawtranslate.com/provisions-on-the-governance-of-the-online-information-content-ecosystem/.

Creemers, Rogier, Paul Triolo, and Graham Webster. 2018. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)." *New America*.

Federal Trade Commission. "Children's Online Privacy Protection Rule ('COPPA')." January 17, 2013. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-ref orm-proceedings/childrens-online-privacy-protection-rule.

GE Appliances. "GE Appliances and Haier Deliver a 'Smarter Home, Better Life' with Transformative, Time- Saving Technologies." News release, January 7, 2019. https:// pressro om.geappliances.com/news/ge-appliances-and-haier-deliver-a-smarter- home-bet ter-life-with-transformative-time-saving-technologies.

Guillou, Céline M. “Privacy Issues in Bankruptcy Sales.” The Privacy Hacker (blog), May 15, 2020. https://www.lexology.com/library/detail.aspx?g=b540a911-a3be-44a4-a49e- 87cf2 ffdff 01.

Haber, Eldar. “The Internet of Children: Protecting Children’s Privacy in a Hyper- Connected World.” *University of Illinois Law Review*, no. 4 (2020): 1209– 48.

Jacob, Indochine Counsel-Steven. 2020. "Data Localisation Requirements in Vietnam." Last Modified December 7, 2020. https://www.lexology.com/library/detail.aspx?g=8dffd587-11b2-4270-a23f-04f432a91e61.

Knockel, Jeffrey, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert. “We Chat, They Watch: How International Users Unwittingly Build up WeChat’s Chinese Censorship Apparatus.” The Citizen Lab, May 7, 2020. https://citizenlab.ca/2020/05/we-chat-they-watch/.

Kokas, Aynne. 2017. *Hollywood Made in China*. Oakland, CA: University of California Press.

Kokas, Aynne. 2020. "Perspective | ‘Mulan’ is a movie about how much Hollywood needs China." *Washington Post*, 2020/09/09/. Accessed 2020/09/10/22:55:59. https://www.washingtonpost.com/outlook/2020/09/09/mulan-is-movie-about-how-much-hollywood-needs-china/.

Kuo, Lily. 2019. "TikTok 'makeup tutorial' goes viral with call to action on China's treatment of Uighurs | TikTok | The Guardian." November 26, 2019. Accessed 2021/04/20/18:20:31. https://www.theguardian.com/technology/2019/nov/27/tiktok-makeup-tutorial-conceals-call-to-action-on-chinas-treatment-of-uighurs.

Lutz, Christoph, and Gemma Newlands. “Privacy and Smart Speakers: A Multi- Dimensional Approach.” *The Information Society* 37, no. 3 (May 2021): 147– 62.

M&A Critique. “ChemChina Buys out Syngenta.” M&A Critique, 2016. https://mnacritique.mergersindia.com/chemchina-buys-syngenta/.

McMahon, Karen. “Drones Provide a Bird’s Eye View.” *Syngenta Thrive* (blog), 2016. https://www.syngenta-us.com/thr ive/production/drones-birdseye-view.html.

Ostrom, Karyn. “New Pilot Program Delivers Innovative Digital Technology.” *Syngenta Thrive* (blog), 2019. https://www.syngenta-us.com/thrive/news/new- pilot-program-delivers-innovative-digi tal-technology.html.

Rafaelof, Emma, Rogier Creemers, Samm Sacks, Katharin Tai, Graham Webster, and Kevin Neville. 2020. "China's 'Data Security Law (Draft)'." Last Modified July 2, 2020, accessed July 2, 2020. http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/.

Smith, Anne Logsdon. “Alexa, Who Owns My Pillow Talk? Contracting, Collaterizing, and Monetizing Consumer Privacy Through Voice- Captured Personal Data.” *Catholic University Journal of Law and Technology* 27 (2018): 186– 226.

Spangler, Todd. 2020. Fortnite Hauls in $1.8B in 2019, Digital Game Revenue up 3% to $109B. *Variety*.

Standing Committee of the National People's Congress 全国人民代表大会常务委员会. 2016. “Zhonghua renmin gongheguo wangluo anquanfa” 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China]. Beijing, PRC: "Zhongguo rendawang" 中国人大网 [China National People's Congress Network].

Syngenta Global. “Our Research Areas: Helping Growers Produce Successful Crops Every Year.” 2021. https://www.syngenta.com/en/innovation-agriculture/research-and-development/our-research-areas.

Syngenta US. “AgriEdge.” Last updated 2020. https://www.syngenta-us.com/agriedge.
Takahashi, Dean. “China Is Approving More Foreign Games, but Not So Many American Ones.” VentureBeat, February 18, 2020. https://venturebeat.com/2020/02/18/china-is- approving-more-foreign-games-but-not-so-many-american-ones/.

Tencent Tech. “Baidu, Haier Partner on Smart Home Products and Platform Development.” Marbridge Daily (blog), March 7, 2018. https://www.marbridgecon sulting.com/marbridgedaily/2018-03-07/article/108657/baidu_haier_partner_on_ smart_home_products_and_platform_development.

The National People's Congress 中国人民代表大会. 2020. "“Shouquan fabu zhonghua renmin gongheguo xianggang tebie xingzhengqu weihu guojia anquanfa”（受权发布）中华人民共和国香港特别行政区维护国家安全法 [(Authorized to promulgate) Law of the Hong Kong Special Administrative Region of the People's Republic of China on Safeguarding State Security]." *XinhuaNet*.

Toh, Michelle. 2020. "Backlash over filming 'Mulan' in Xinjiang 'generated a lot of issues,' admits Disney." Last Modified September 11, 2020. https://www.cnn.com/2020/09/11/media/disney-mulan-xinjiang-intl-hnk/index.html.

Tully, Shawn. “This Agriculture Giant Is Bringing in the Drones to Modernize Farming from Cornfields to Vineyards.” *Fortune*, June 19, 2018. https://fortune.com/2018/06/19/syngenta-chemchina-drones-farming/ .

国家互联网信息办公室令 guojia hulianwang xinxi, bangongling. 2019. "《网络信息内容生态治理规定》全文 wangluo xinxi neirong shengtai zhili guiding." *人民网 renminwang*.

Yu, Xie. “Haier Has a Plan to Turn Around Its US$5.6 Billion GE Appliances Unit.” *South China Morning Post*, October 23, 2017. https://www.scmp.com/business/ companies/article/2116486/chinas-haier-has-plan-help-continue-turnaround-ge- appliances.

Zakarin, Jordan. “Marvel to Release Special Chinese Cut of ‘Iron Man 3.’” The Hollywood Reporter, March 29, 2013. https://www.hollywoodreporter.com/news/general-news/chinese-iron-man-3-cut-431747/.

Zhu, Julia. “The Personal Information Protection Law: China’s Version of the GDPR?” *Columbia Journal of Transnational Law*, February 14, 2022. https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr.