NOVEMBER 5, 2019

PREPARED TESTIMONY BEFORE THE SENATE JUDICIARY SUBCOMMITTEE ON CRIME AND TERRORISM[1]

Hearing on "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors"

BY

Kara Frederick

Fellow, Technology and National Security
Center for a New American Security

[1] In addition to new material, this testimony includes original content from the witness's previously published work and media commentary.

I. Key Observations and Assessments[2]

Chairman Hawley, Ranking Member Whitehouse, distinguished members of the subcommittee, thank you for the opportunity to discuss a topic of critical importance to the United States. I want to begin with a few observations:

1) **Americans face *systemic risk* when using platforms operating in or owned by companies in countries with a history of cyber espionage, forced tech transfer, and a lack of rule of law.** Without the same system of checks and balances against misuse we have in the United States, U.S. citizens are at high risk for data exploitation via these platforms. In addition to an established precedent of IP theft and espionage against the United States, private Chinese technology companies' ability to resist the Chinese government is highly circumscribed at best. This is due in part to the Chinese government's deliberate blending of the public and private digital landscape through Article Seven of China's 2017 National Intelligence Law, where Chinese organizations and citizens are compelled to cooperate with "state intelligence work."[3] China's much-examined 2017 Cybersecurity Law and subsequent updates also bolster this tactic.[4] As public policy researchers noted last year, these laws "[entail] strict provisions requiring data to be housed inside China, as well as spot inspections and even black-box security audits."[5] If a company stores U.S. data overseas, that data may be subject to similar foreign legislation. "Country-agnostic" approaches (or, relatedly, vendor-neutral approaches to building out critical infrastructure like next generation wireless technology)—while rhetorically expedient—do not strike at the heart of these systemic issues.[6]

   Further, American lawmakers and citizens possess even less insight into the data security practices of foreign-owned technology companies than they do businesses in the United States. The lack of granularity provided on real-time data collection, levels of access, storage, server locations, and third-party partnerships present a national security risk. In the case of TikTok, David Carroll, writing in Quartz in May 2019, asserted that an earlier version of TikTok's privacy policy allowed data on the app

---

[2] A portion of these observations are derived or pulled directly from a paper written exclusively by the witness and dated October 2019, "Reclaiming Cyber Governance as a Bulwark Against—and Not a Tool of—Illiberalism" for the U.S. government's Congressionally-mandated Cyber Solarium Commission. Expected release is 2020.

[3] "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Further, the CCP's September 2019 decision to send Chinese officials to work in 100 private companies in Hangzhou continues to muddy the waters between public and private industry.

[4] "Translation: China's New Draft 'Data Security Management Measures,'" *New America*, May 31, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/; https://www.zdnet.com/article/chinas-cybersecurity-law-update-lets-state-agencies-pen-test-local-companies/; and https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[5] Ibid.; "Breakingviews - America can define down China's harsh cyber rules," *Reuters*, April 2, 2019, https://www.reuters.com/article/us-usa-trade-china-breakingviews/breakingviews-america-can-define-down-chinas-harsh-cyber-rules-idUSKCN1RE08F; and "China's Ambitious Rules to Secure 'Critical Information Infrastructure," *New America*, July 14, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-ambitious-rules-secure-critical-information-infrastructure/.

[6] Samantha Hoffman, "Engineering global consent: The Chinese Communist Party's data-driven power expansion," Policy brief Report No. 21/2019 (Australian Strategic Policy Institute, October 2019), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT.

to be shared with "with any member or affiliate of [its] group" in China before the policy's revision in February 2019.[7] While TikTok claims to store its data in the United States as of today, its Beijing-headquartered parent company, ByteDance, is subject to the Chinese legislation noted above. In addition to this legislation, technical vulnerabilities in systems built and owned by Chinese companies abound. These can include much-discussed "backdoors" in code that would allow the Chinese government access to third party systems and security flaws hidden in a programming vulnerability, or "bugdoors"—flaws could even be introduced later via a software update.[8]

2) **China is exporting its values embedded in the technology itself and legal frameworks to the world.** Leaked documents from TikTok indicate the company censors content on Tiananmen Square and Tibetan independence, and *possibly* reporting on the Hong Kong protests and the imprisonment of approximately 1 million Uighurs in Xinjiang detention camps.[9] Not only China exporting technology, particularly AI-related surveillance tech, but the Chinese "party-state" is also transmitting the laws and policies that govern its use. For instance, Vietnamese officials were trained in and attempted to implement a cybersecurity law modeled after China's version of the legislation in 2018. This draft law contained strict data storage provisions (which gives access to a government "task force"), a mandate to open offices in Vietnam if requested by Vietnam's Public Security Ministry, and overarching definitions of content. It is also expanding that access through its legislation: China's full "internet security plan," encompassing a soon-to-be-implemented 2020 Foreign Investment Law, will no longer render foreign-owned companies in China exempt from the Cybersecurity Law.[10] Effectively, any data on communications networks in China will be soon be subject to the Chinese Cybersecurity Bureau's scrutiny, without requiring an official request. This ability to access more data from more sources lays the groundwork for its exploitation.[11]

3) **Private companies play an outsized role in this environment due to their sustained and unfettered access to a high volume and variety of personal data—behavioral and biometric—with high commercial value.** A May 2019 survey indicated almost half (46%) of 18-24 year olds accept tech privacy agreements without reading a single word.[12] This bargain has led to private tech companies' often overwhelming access to consumer data, such as when IBM scraped millions of photos from unwitting citizens using photo hosting site Flikr at the beginning of this year.[13]

---

[7] David Carroll, "Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?" qz.com, May 7, 2019, https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat.
[8] Kara Frederick, "The 5G Future Is Not Just About Huawei," Foreignpolicy.com, May 3, 2019, https://foreignpolicy.com/2019/05/03/the-5g-future-is-not-just-about-huawei/.
[9] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing; https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/
[10] "China's New Cybersecurity Program: NO Place to Hide," *China Law Blog*, September 30, 2019. https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html.
[11] This section is taken directly from the witness's unpublished report for the U.S. Cyber Solarium Commission.
[12] Kim Hart, "Privacy policies are read by an aging few," Axios.com, February 28, 2019, https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html.
[13] Olivia Solon, "Facial Recognition's 'dirty little secret': Millions of online photos scraped without consent," NBC News, March, 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921

4) **The digital environment is growing more complex**. The strategic intent of bad actors is increasingly difficult to delineate, and emerging technologies are exacerbating existing threats. Emerging technologies, particularly machine learning, will give malign actors the ability to turn data into insights. In addition, the strategic intent of nation-state actors, cybercriminals, and hacktivists is increasingly intertwined, heightening the chaotic nature of the landscape. Protecting the United States against these supercharged threats from various attack vectors will only get harder.

5) **Solutions are overdue. If democratic societies do not establish the rules of the road for data security and privacy protections, authoritarians will do it for us.** By next year alone, approximately 30 billion devices will be connected to the internet, and by 2025, almost five billion people will have access to the web.[14] This amounts to a huge attack surface for cybercriminals, adversarial nation-states, and other bad actors to both wreak havoc and set their own standards.

II. Recommendations[15]

The advent of the internet and social media promised to wrench control of information from the hands of a few and distribute it to the many, to air marginalized perspectives, to elevate new views in a meritocracy of ideas, and even to propagate a more open society. Decentralized applications and low barriers to entry across the digital space acted as great levelers. Yet, increasingly, that vision is under threat. As China attempts to impart its authoritarian values on the United States, private industry and the U.S. government must develop a set of solutions to push back.

1) **Congress should mandate interagency import reviews of information and communications technologies against a criteria that encompasses the likelihood of systemic risk (e.g. lack of the sufficient rule of law protections, a free press, an independent judiciary, and recourse against government demands for private data, etc).** This criteria should serve to exclude untrusted private sector vendors and governments from collecting U.S. data on the basis of a series of risk factors or key indicators. The State Department's September 2019 draft guidance for the export of hardware, software, and technology with surveillance capabilities is a good start point.[16] The DoS document's due diligence and red flag considerations can be extended to include the following key criteria: *Data aggregation with established intent of political or social control; Significant surveillance technology investments abroad; Significant evidence of government subsidizing private industry; A track record of exporting to regimes consistently ranked low on Freedom House, World Bank, etc., rankings or those found to have committed gross violations of human rights as defined in FAA 1961.*

---

[14] Kara Frederick, "The Rise of Municipal Ransomware," City-Journal.org, September 3, 2019, https://www.city-journal.org/ransomware-attacks-against-cities.

[15] A portion of these recommendations are derived or pulled directly from a paper written exclusively by the witness and dated October 2019, "Reclaiming Cyber Governance as a Bulwark Against—and Not a Tool of—Illiberalism" for the U.S. government's Congressionally-mandated Cyber Solarium Commission. Expected release is 2020.

[16] This draft guidance is based on based on privacy violations laid out in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR)—"Draft U.S. Government Guidance For The Export Of Hardware, Software And Technology With Surveillance Capabilities And/Or Parts/Know-How," *U.S. Department of State*, September 2019, https://www.state.gov/wp-content/uploads/2019/09/DRAFT-GUIDANCE-FOR-THE-EXPORT-OF-HARDWARE-SOFTWARE-AND-TECHNOLOGY-WITH-SURVEILLANCE-CAPABILITIES.pdf.

2) **Lawmakers should enshrine data protections and incentivize transparency within the government and the private sector.** For the government, that means maintaining transparency by keeping the public informed on how their personal information is being used and protected. Clear policies and limits should be articulated around data retention, such as limited tolerance for storing data indefinitely. Classify biometric data as "sensitive data" and enshrine protections around this data, including limited interoperability with other commercial and government systems. In accordance with NIST guidelines, any identity management systems must be secure and reliable, based off proper standards and measurement.[17] Enforce data protection inspections and oversight among agreed-upon parties.[18] Congress should also explore a national data protection framework as "baseline privacy protections."[19] Private companies should invest a substantial portion of engineering capacity to developing technical privacy solutions, such as protecting biometric data on the back end. They can also further explore new ways to create systems that promote user control of data by examining new navigation protocols.[20]

3) **Tech companies should adopt a set of rules, norms, and guiding principles for the use of their tech globally (and for interfacing with authoritarian regimes) that won't tip the scale in favor of repression.** Given this systemic risk and contest, American private companies should treat U.S. national security as a strategic imperative and provide regular updates on the guardrails that implement to Congress. If deficient, the Magnitsky Act and Commerce Department Entity listings provide enforcement mechanisms for the abuse of this technology by individual and corporate actors.

4) **Frontload investment in securing digital infrastructure from the outset**. Critical U.S. infrastructure is vulnerable to IP theft, weakened data privacy, hacking, and other disruptions of the digital systems Americans take for granted. The U.S. government can stay competitive by prizing network and data security against nation-states and other actors with a track record of attacking U.S. systems.[21]

I look forward to taking your questions.

---

[17] "NIST Testimony: Facial Recognition Technology (FRT)," *NIST*, March 22, 2017, https://www.nist.gov/speech-testimony/facial-recognition-technology-frt.
[18] "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," February 2018, https://arxiv.org/pdf/1802.07228.pdf.
[19] Nuala O'Connor, President and CEO of the Center for Democracy & Technology, "Consumer Data Privacy: Examining Lessons from the European Union's General Data Protection Regulation and the California Consumer Privacy Act," Statement to the Committee on Commerce, Science, and Transportation, U.S. Senate, October 10, 2018, https://cdt.org/files/2018/10/2018-10-09-FINAL-Nuala-OConnor-Written-Testimony-Senate-Commerce.pdf.
[20] "Google Draws House Antitrust Scrutiny of Internet Protocol," *WSJ*, September 29, 2019, https://www.wsj.com/articles/google-draws-house-antitrust-scrutiny-of-internet-protocol-11569765637?mod=hp_lead_pos6.
[21] Kara Frederick, "The 5G Future Is Not Just About Huawei," Foreignpolicy.com, May 3, 2019, https://foreignpolicy.com/2019/05/03/the-5g-future-is-not-just-about-huawei/.