Senate Judiciary Committee
"How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors"
Questions for the Record
November 13, 2019
Senator Amy Klobuchar

Questions for Kara Frederick, Center for a New American Security

You testified about the broad range of data that private companies can collect from Americans, including pictures, location data, and social media activity.

- How can this information, like ad targeting data, be used by malicious actors who are attempting to influence an American election?

Answer:
Such data collection can lead to the creation of digital, behavioral profiles for specific users. These profiles can be used to conduct microtargeting campaigns aimed at more effective political influence. For instance, Google allowed advertisers to target its "left-leaning" or "right-leaning" users in 2016. Once users are identified as "left-leaning" or "right-leaning" on media platforms, political interest targeting can open the door for more malicious targeting efforts.[1] For example, future scenarios include the use of layered data like location patterns and ideological preferences to determine if a partisan user lives in a swing district. With this information, a malicious actor could feasibly serve them tailored, false information at specific periods of time to attempt to influence voting behavior during a critical timeframe (e.g. false information about voting locations or false information about a candidate's likelihood of victory just before the polls close).[2]

I introduced the Honest Ads Act with Chairman Graham to help prevent foreign actors from influencing our elections by ensuring that political ads sold online are covered by the same rules as ads sold on TV, radio, and satellite.

- Do you agree that increased transparency can help protect our elections from cyber threats?

Answer:

---

[1] Google, "Security and Disinformation in the U.S. 2016: What We Found," October 30, 2017, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/google_US2016election_findings_1_zm64A1G.pdf via https://www.blog.google/outreach-initiatives/public-policy/security-and-disinformation-us-2016-election/; and Kara Frederick, "The New War of Ideas: Counterterrorism Lessons for the Digital Disinformation Fight," *CNAS*, June 3, 2019, https://www.cnas.org/publications/reports/the-new-war-of-ideas.

[2] Kara Frederick and Paul Scharre, "Digital Freedom and Repression," *CNAS*, June 14, 2019, https://www.cnas.org/publications/video/digital-freedom-and-repression; and Miles Brundage, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," *Future of Humanity Institute, University of Oxford*, February 2018, https://arxiv.org/pdf/1802.07228.pdf.

Increased transparency in the form of identifying and labeling foreign, state-run bots, the provenance of ads, etc. can provide users with more information to make their own judgements during the electoral process. This type of increased transparency can help mitigate the effect of foreign influence campaigns on individual members of the electorate.

United States Senate Judiciary
Subcommittee on Crime and Terrorism

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

Questions for the Record for Kara Frederick
Submitted by Senator Richard Blumenthal
November 7, 2019

1. The Beijing-based ByteDance, which owns TikTok, told this Subcommittee in a letter that it is not beholden to the Chinese government. It stated that "no governments, foreign or domestic, direct how we moderate TikTok content" and that all U.S. user data is stored in America and Singapore. However, its letter and public statements tell us little about what ByteDance would do in the face of Chinese government pressure.

   According to Reuters, the Committee on Foreign Investment in the United States is considering behavioral and structural conditions on how ByteDance operates TikTok. Among the risks CFIUS can consider is whether a deal gives foreigners access to sensitive information about Americans. It is for this reason CFIUS required a Chinese firm to divest Grindr, a popular LGBTQ dating app, over fears its users were vulnerable to espionage and persecution by the China government.

   a. ByteDance has told us that the company and its U.S. users are out of reach of the Chinese government. Should we believe ByteDance? Does storing data in U.S. data centers actually prevent the Chinese government from gaining access to Americans' data? What would happen to ByteDance if it said 'no' to a Chinese request?

      Answer: United States policymakers cannot assume ByteDance, a private Chinese company headquartered in Beijing, is out of reach of the Chinese government. The relationship between private Chinese companies and the Chinese government is increasingly inscrutable due to the broad nature and uneven implementation of Chinese cybersecurity, intelligence, and investment laws and standards. It is possible that ByteDance itself does not know if and how these laws—ones that stand to govern data storage and handling—will be implemented. For example, the Chinese government deliberately blended 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."[1] Also, China's 2020 Foreign Investment Law appears to no longer render foreign-owned companies in China exempt from the 2017 Cybersecurity Law.[2] If executed as written, any

[1] Murray Scot Tanner, "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.
[2] Steve Dickinson, "China's New Cybersecurity Program: NO Place to Hide," *China Law Blog*, September 30,

data on communications networks in China could be subject to the Chinese Cybersecurity Bureau's scrutiny, without requiring an official request.

Storing data in the United States can mitigate, but not prevent, the Chinese government from gaining access to Americans' data. The location of servers where data is stored is not the only factor to consider in terms of data access. Laws, policies, and the "leverage" and influence the Chinese government has over *people* with potential access to data can also play a role in how data is handled.[3]

If ByteDance refuses to comply with government requests for data by the Chinese government, it faces a lack of clear recourse. China does not have the United States' independent judiciary to hear its defense or a free press to amplify its concerns. The 2016 encryption dispute between Apple and the FBI over the San Bernardino attacks offers a contrast to the Chinese model of corporate governance and public-private relationship, in that a private U.S. technology company was able to resist the U.S. government's request and subsequent court order for user data through an appeal.[4]

b. Are there any measures that CFIUS could impose on Chinese firms collecting information about Americans that would provide *real* assurances that the data will not end up in Chinese government hands?

Answer: Because CFIUS cannot enforce clear, focused, and predictable implementation of laws and standards written in China, it will struggle to *ensure* American data will not end up in Chinese government hands. Ultimately, the systemic differences outlined above put pressure on the ecosystem surrounding data—the private firms, the people in them, etc.—and preclude guaranteed assurances. CFIUS can take measures to deter the exploitation of U.S. user data by imposing costs, as it does today (e.g. Grinder divestment). Additionally, the U.S. government and U.S. private sector can work together to encourage good cyber hygiene measures and infrastructure security surrounding systems that store American data—in addition to data protections—so that Americans' data is less vulnerable at the outset.

c. How would you recommend that joint ventures or acquisitions with Chinese firms are not used for spying on U.S. consumers?

2019.
https://www.chinalawblog.com/2019/09/chinas-new-cybersecurity-program-no-place-to-hide.html; and Rogier Creemers, Paul Triolo, and Graham Webster, "Cybersecurity Law of the People's Republic of China," *New America*, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[3] Drew Harwell and Tony Romm, "Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses," *The Washington Post*, November 5, 2019, https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[4] "The Apple-F.B.I. Case," *The New York Times*, 2016, https://www.nytimes.com/news-event/apple-fbi-case.

Answer: To help prevent spying on U.S. consumers, Americans' data should be enshrined with clearly articulated data protections, starting at the earliest use of the U.S. platform (where possible). For instance, if U.S. systems are collecting data beyond subscriber data, this data should be time-limited and not stored indefinitely. Any biometric data should be classified as "sensitive data" and handled accordingly (e.g. compliant with NIST identity management system guidelines, standards, and measurement). Such protections should remain or be elevated if the U.S. company in question takes part in a joint venture or acquisition with a Chinese firm.

2. As we know, Chinese hackers carry out massive campaigns to steal intellectual property and trade secrets from U.S. companies, amounting to billions of dollars of losses to our economy. In 2015, the Obama administration was prepared to exercise an executive order that would authorize sanctions against companies or individuals that profit from this cyber theft, including state-owned enterprises and senior Chinese officials.

   Using the threat of U.S. sanctions, President Xi Jinping and President Obama agreed that

neither of their countries would "conduct [nor] knowingly support cyber-enabled theft … including trade secret or other confidential business information." After they reached this agreement, cybersecurity companies recorded a steep decline in Chinese attacks against U.S. companies that continued into 2016. However, in the past three years, cybersecurity companies have reported Chinese hackers have resumed their campaigns.

a. What is the reason that the U.S.-Chinese hacking agreement did not hold?

Answer: I believe this question would best be directed to the United States intelligence community.

b. The Trump administration has focused on indictments against Chinese individuals, corporations, and state-owned enterprises, rather than targeted sanctions. Is there any evidence that indictments were more effective than targeted sanctions?

Answer: An accurate measure of the effectiveness between the two approaches is beyond my range of expertise.

3. U.S. intelligence and law enforcement agencies have warned that Russia, Iran, and others have sought to interfere in the 2020 presidential campaigns using disinformation and hacking. Until recently, China has been less visible about using Facebook and Twitter to meddle in our political affairs. This is despite the Chinese Communist Party's considerable success at shaping public opinion at home, thanks to a blend of online censorship, patriotic trolls, and directives to state-run media.

a. Twitter stated that it would ban China Daily and other state-backed publication from advertising in response to its propaganda against Hong Kong protestors, a step that Facebook was unwilling to take. What is Chinese state media's role in foreign influence campaigns?

Answer: From an open-source perspective, the Chinese "party-state" appears to be increasing its support of foreign influence campaigns, in addition to diversifying its tactics. Previous state-controlled attempts to influence political outcomes within and outside China's borders include identifying and targeting specific, high-level individuals or propagating pro-regime messaging through its 50 cent army.[5] However, recent influence campaigns in Hong Kong and the 2018 Taiwanese presidential election indicate Chinese state-supported actors are making use of tactics to sow discord in the internal, domestic politics of democratic nations.[6] Beyond the open-source reporting cited here, the United

[5] Henry Farrell, "The Chinese government fakes nearly 450 million social media comments a year. This is why," *The Washington Post*, May 19, 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/.

[6] Steven Lee Myers and Paul Mozur, "China Is Waging a Disinformation War Against Hong Kong Protesters," *The New York Times*, August 12, 2019, https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protests-china.html; and Chris Horton, "Specter of Meddling by Beijing Looms Over Taiwan's Elections,"

States intelligence community can likely offer more granularity on the tactics, techniques, and procedures used by Chinese government actors in foreign influence campaigns.

b. Did Twitter take the right step in banning China Daily?

Answer: I believe identifying and removing malign, ***foreign, state-supported*** influence campaigns of verified disinformation from U.S. platforms is an appropriate step U.S. companies can decide to take.

The New York Times, November 22, 2018, https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html.