Computer & Communications Industry Association
Tech Advocacy Since 1972

NATIONAL SECURITY ISSUES POSED BY HOUSE ANTITRUST BILLS[1]

The United States is at a critical inflection point in its innovation race with China and the economic, geopolitical, and national security stakes could not be higher. Chinese President Xi last year announced his government would invest $1.4 trillion by 2025 to overtake the United States in key technology fields, and as of 2018, nine of the top twenty technology firms by market valuation are now based in China. In response to this ongoing threat, the Senate recently passed an ambitious proposal to empower U.S. technology research and development, particularly in key emerging technologies like artificial intelligence, quantum computing, and cloud services.

However, the House of Representatives is considering several bills targeting leading U.S. technology firms with sweeping provisions that are in serious tension with the overall U.S. national innovation strategy to combat China and other adversaries. In fact, these bills contain provisions that, as drafted, may inadvertently undermine U.S. national security by transferring sensitive data to adversaries and granting foreign competitors access to U.S. digital platforms, hardware, and software. Additionally, these bills would weaken the U.S.'s ability to counter foreign cyber attacks, espionage, influence and surveillance efforts. Furthermore, only a small group of U.S. tech companies are in scope under these bills, while a much larger set of foreign rivals in China, Russia, and other markets are entirely exempt from the legislation.

The House Judiciary Committee recently approved the following bills without conducting any impact assessment or meaningful debate about the potential impact on U.S. national security:

- The "American Innovation and Choice Online Act" (H.R. 3816), which contains provisions requiring a handful of leading tech companies to provide "access and interoperability" to their platforms, software and hardware, including to foreign entities, as well as "nondiscrimination" provisions that could restrict activities to protect against malicious activity.
- The "Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act" (H.R. 3849), which contains provisions requiring a handful of leading U.S. tech companies to allow data portability and interoperability, including to foreign entities.
- The "Platform Competition and Opportunity Act" (H.R. 3826), which would impose severe restrictions on mergers and acquisitions by a handful of leading U.S. technology companies and not on foreign rivals.
- The "Ending Platform Monopolies Act" (H.R. 3825), which would prohibit a handful of leading U.S. tech companies from offering certain products or services on their platforms, essentially requiring these companies to sell off parts of their businesses, putting them at a significant disadvantage versus global competitors.

[1] The analysis in this paper has been prepared by King & Spalding LLP on behalf of the Computer & Communications Industry Association.

Before proceeding with these bills, Congress should engage its national security committees to solicit briefings and technical assistance from U.S. intelligence, counterintelligence, and foreign policy agencies. These stakeholders could offer important insights on the national security implications of the House bills as well as other legislative proposals to regulate competition in the technology industry.

As detailed below, these bills could negatively affect U.S. national security by:

1. Risking the misuse of U.S. data and intellectual property by foreign actors;
2. Reducing the effectiveness of data streams to law enforcement;
3. Weakening efforts to combat foreign influence and misinformation;
4. Impeding the enforcement of robust cybersecurity policies;
5. Giving foreign companies advantageous treatment without requiring reciprocity; and
6. Undermining U.S. tech leadership.

Risking Misuse of U.S. Data and Intellectual Property by Foreign Actors

Both H.R. 3816 and H.R. 3849 include a number of sweeping provisions on data portability, interoperability, and access to U.S. technical infrastructure. These broadly drafted provisions could have the unintended consequence of requiring U.S. online platforms to share sensitive or protected user data and IP with other companies, and could lead to forced IP transfers to foreign competitors and foreign entities controlled by U.S. adversaries. For example, the interoperability requirements in H.R. 3816 would force U.S. companies to allow foreign rivals to "connect to any product or service" and "access or interoperate with … platform, operating system, hardware and software features" offered by U.S. companies. This requirement to grant competitors direct access to U.S. digital infrastructure – including app stores, marketplaces, search engines, and other interfaces – is not accompanied by meaningful security requirements or safeguards regarding the scope of that access. This could entitle foreign companies, including those that are beholden to our adversaries, to seek access to source code associated with U.S. platforms, and to U.S. users' data and behavioral insights via those platforms.

Reducing the Effectiveness of Threat Information to Law Enforcement

Major U.S. technology companies and online platforms work with U.S. law enforcement, military, and intelligence agencies to combat a variety of national security and criminal threats. The head of U.S. Cyber Command in 2020 discussed the importance of the U.S. government's engagement with the tech industry, noting that "many leading U.S. companies find themselves on the frontlines of competition in cyberspace. Working collaboratively where we can allows us to improve collective defense and stay a step ahead of our adversaries."

The nature and scale of these platforms gives them a broad and deep view of the threat landscape. This allows those companies to secure U.S. data and infrastructure against foreign threats with an agility, speed and thoroughness that is not feasible for smaller, fragmented companies that have limited apertures. The critical missions of national security and law enforcement agencies, of course, also benefit from this security proficiency. Not only are the threats more rapidly detected and mitigated, but trend and threat analysis can be quickly shared with these agencies in multiple matured fora that have evolved over the last 10 years. This also means that government agencies can more effectively and confidently use

the legal tools available to investigate threats posed by hostile foreign adversaries, including terrorists, proliferators, spies, and cyber actors.

At a moment in history when it has never been more clear that cyber threats are very real and can impact the daily operation of the economy as well as essential services, the provisions in the House bills that seek to reduce the size, scale, and integration of a handful of leading U.S. tech firms, especially H.R. 3825 and H.R. 3816, could significantly hinder the ability of the agencies to fulfill their missions to defend against such threats. A scattered group of smaller, isolated platforms with scant perspective of the threats they each face, and fewer resources, will be unable to engage in the same level of threat detection, investigation, mitigation and information sharing. The loss to U.S. government efforts will be further significantly compounded if, as should be expected, foreign companies step in to take at least some of customers previously served by U.S. companies. Not only will these companies be less inclined to work with U.S. agencies, they will be outside the scope of statutory legal authorities granted to U.S. agencies to compel the production of information.

Weakening Efforts To Combat Foreign Influence and Misinformation

The most recent Annual Threat Assessment from the Office of the Director of National Intelligence notes China is actively intensifying its efforts to influence U.S. politics "to promote its policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China on such issues as religious freedom and the suppression of democracy in Hong Kong." These efforts often take place via U.S. online platforms and have become increasingly antagonistic and dangerous, with U.S. platforms leveraging their threat analysis data across products to take action on thousands of influence operations. This year alone, several thousand accounts linked to Chinese, Russian, and Iranian influence efforts on U.S. platforms were terminated. The "anti-discrimination" provisions of H.R. 3816 could hamper the ability of U.S. technology companies to restrict and police Chinese competitors that may serve as vectors of Chinese misinformation, both by halting the collection of cross-product intelligence about these operations and by requiring the disclosure of this intelligence in some cases to untrusted third parties. And if U.S. technology companies are fragmented, it is likely that China—not to mention Russia and other adversaries—would be emboldened to pursue even more aggressive influence and misinformation tactics. State-sponsored influence and misinformation operations cannot be effectively countered by fragmented U.S. companies that do not have the scale and security resources to analyze and respond to evolving threats.

Impeding the Enforcement of Robust Cybersecurity Policies

China has also become increasingly aggressive in its cyber-espionage operations, leading the United States, EU, UK and NATO to issue statements in July "exposing and criticizing the PRC's malicious cyber activities," with the United States formally attributing several major recent hacks to Chinese-affiliated hackers. In addition, the FBI, NSA, and CISA recently issued a joint Threat Alert warning that "Chinese state-sponsored cyber actors aggressively target U.S. and Allied political, economic, military, educational, and critical infrastructure personnel and organizations to steal sensitive data, emerging and key technology, intellectual property, and personally identifiable information." U.S. technology companies and platforms have led the way in innovative cybersecurity policies and solutions to detect and thwart foreign cyberattacks, both on their core operations and in the broader ecosystems that they manage.

However, the access and interoperability provisions in H.R. 3816 and H.R. 3849 may impede U.S. technology companies from enforcing their robust cybersecurity policies regarding third parties, both by deterring the collection of cross-platform intelligence, and by requiring such data to be shared in a way that decreases the value of intelligence and increases security threats related to such intelligence. This could unintentionally weaken the ability to block malicious foreign activity on the web or via apps, and ultimately enable China and other adversaries to more easily exploit U.S. platforms to disseminate Trojan Horse apps or other compromised technologies. If the key components of the digital architecture underlying the global economy are subject to compromise and espionage, it puts the United States and our allies at risk. Furthermore, U.S. technology companies often use economies of scale, including by aggregating threat data from across platforms and leading technical talent, to create the most advanced methods of data protection. The provisions of the bills aimed at diminishing those economies of scale, such as the restrictions on operations in H.R. 3825, prohibitions on integrated services in H.R. 3816, and the limits on acquisitions in H.R. 3826, over time could hamper these data protection efforts and leave the underlying data collected by U.S. technology firms more vulnerable.

Giving Foreign Companies Advantageous Treatment Without Requiring Reciprocity

The House Judiciary bills impose a series of restrictions on leading U.S. tech companies, but do not place any similar restrictions on foreign competitors. Most important from a national security perspective, the bills would make it easier for Chinese and other foreign competitors to acquire U.S. technology. For instance, the limits on acquisitions imposed in H.R. 3826 would apply only to a handful of leading U.S. tech companies. This would better position foreign companies to acquire innovative U.S. companies, enabling foreign countries to own key technologies and IP that are currently held in the United States. Foreign companies would also benefit from reduced competition and prices when bidding on U.S. technologies. Similarly, the restrictions on the operations of a handful of leading U.S. tech firms in H.R. 3825 would likely result in these companies divesting parts of their integrated product lines, potentially allowing foreign companies to acquire these divested assets and lines of business. Indeed, other covered U.S. companies would likely be unable to acquire these divested assets, significantly lowering the price that foreign companies would need to pay to acquire them.

In addition, the "access and interoperability" and the "anti-discrimination" provisions of H.R. 3816 apply only to a handful of leading U.S. companies, while foreign platforms won't be obligated to provide the same treatment to U.S. products and services. Provisions in H.R. 3816 and H.R. 3825 also limit the ability of large U.S. companies to offer integrated products, while foreign firms are fully exempt from any comparable regulatory oversight. This would improve the competitive position of foreign companies, who already are leading competitors and who would be able to benefit from the scale and integration advantages that are no longer available to major U.S. platforms. Finally, U.S. companies will face a series of restrictions, delays, and prohibitions on bringing new integrated technologies to market, and foreign rivals will face none of these obstacles - making it more likely that users of U.S. companies shift their data away from less agile U.S. services and to integrated services offered by foreign rivals.

Undermining U.S. Technology Leadership

While the United States has long served as the global leader in technology, China has made no secret of its efforts to achieve technological superiority in many key areas, including semiconductors, artificial intelligence, 5G, digital services, and cloud data storage and management. Through heavy subsidization and protection of its companies from foreign competition, China now has nine of the world's top 20 technology giants. The CCP believes that these long-term technology investments not only will allow the country to perfect the surveillance state inside its borders, but also to achieve military and economic dominance against Western countries. Economies of scale are significant for the innovation race. In other words, the breadth of U.S. online platforms is an important strategic advantage in our technological arms race with China. The National Commission on AI put it simply: "more and better data, fed by a larger consumer/participant base, produce better algorithms, which produce better results, which in turn produces more users, more data, and better performance—until, ultimately, fewer companies will become entrenched as the dominant platforms. If China's firms win these competitions, it will not only disadvantage U.S. commercial firms, it will also create the digital foundation for a geopolitical challenge to the United States and its allies."

As noted above, the House bills' operative provisions include general limits on acquisitions, broad conflicts of interest procedures designed to disaggregate platforms, and data interoperability requirements that might give foreign competitors broader access to U.S. data than they previously enjoyed. Collectively, these bills could undermine those critical economies of scale and thus diminish U.S. competitiveness in this crucial area. U.S. tech leaders targeted by the House bill are the same companies who are the primary investors in R&D in many critical sectors and rank among the top corporate investors in R&D globally. Passage of these bills would undercut the United States' ability to continue to lead on global tech competitiveness and tech R&D; alternatively, these bills would restrict and/or dismantle the most successful U.S. tech companies and cede U.S. tech leadership to foreign competitors.