The Heritage Foundation

LEGAL MEMORANDUM

No. 311 | OCTOBER 27, 2022

EDWIN MEESE III CENTER FOR LEGAL & JUDICIAL STUDIES

Big Tech's National Security Red Herring

Michael J. Ellis and Kara Frederick

KEY TAKEAWAYS

Big Tech companies built their monopolies partly through dependence on China and collaboration with the Chinese Communist Party.

Now Big Tech is arguing that antitrust reforms that target their abuse of power threaten U.S. national security.

Policymakers should not fall for this claim; competition, not Big Tech monopolies, will produce the innovation that America needs.

Congress will soon consider two significant reforms to disrupt the Big Tech companies whose totalitarian behavior threatens freedom of speech and open discourse online. Earlier this year, the Senate Judiciary Committee reported out the American Innovation and Choice Online Act (AICOA, S. 2992),[1] which would prohibit Big Tech companies from giving an advantage to their own products on the platforms they operate, and the Open App Markets Act (S. 2710),[2] which would open Apple and Google's mobile app stores to competition from third-party software developers. Both bills garnered bipartisan support in committee, and the Biden Administration has announced its support for AICOA, leading to the possibility that one or both may become law.[3]

In response, Big Tech companies have launched a lobbying campaign to oppose the two bills. One goal of this campaign is to shift the legislative debate away

from the substance of the antitrust reforms and into new areas, including the claim that antitrust reform will harm U.S. national security. Through open letters, op-eds, and speeches, dozens of former U.S. national security officials have argued that any antitrust reforms will harm the United States in its strategic competition with China. At a high level, they argue that antitrust reforms will prevent American companies from serving as "national champions," which will lead to the dominance of Chinese tech giants.[4] More specifically, they argue that the antitrust reform bills now under consideration will open the door to cybersecurity threats and misinformation from malign foreign actors.

A closer look reveals two things:

- These arguments are smoke-and-mirrors attempts to distract from the anticompetitive conduct of Big Tech companies, and

- There is little connection between the substance of the proposed antitrust reforms and their opponents' purported national security concerns.

These national security arguments are misplaced. American Big Tech companies are not and never will be the equivalents of China's tech "national champions" like Alibaba and Tencent. Quite the opposite: As we explore in greater detail below, some Silicon Valley giants like Apple built their market position through partnerships with the Chinese Communist Party (CCP) that are nearly impossible for them to end. Through their dependence on Chinese manufacturing and, in many cases, the Chinese consumer market, Big Tech companies have subjected themselves to Chinese government coercion, including requirements that they share technology and the personal data of their users with the CCP. These same Big Tech companies are also unlikely to drive future innovation, as their dominant market position allows them to deprioritize research and development, kill innovation from start-ups, or acquire new entrants to reduce competition.

Moreover, many of the reforms under consideration—including AICOA and the Open App Markets Act—have little to do with the arguments raised by former national security officials. When Congress and executive branch policymakers consider antitrust reforms, they should look past specious national security arguments and consider the reforms on their merits alone.

Big Tech Monopolies Hurt America's Competitiveness Against China

Silicon Valley's goliaths have generated massive amounts of wealth in the United States, and their products have created enormous value, but no one should mistake these companies for American equivalents of China's tech "national champions." Chinese companies like Alibaba, Baidu, Tencent, and Huawei take direction from the CCP on the conduct of their business operations and receive benefits from the CCP that include subsidies and low-cost capital. In return, Chinese companies carry out economic espionage campaigns to give themselves competitive advantages and coordinate their investment in key technologies.[5] In our freer economy and under our current corporate governance practices, the United States government does not exercise a similar degree of control over large U.S. technology companies. No matter their size, those companies do not play a role similar to that of China's tech champions in the strategic competition between the United States and China.

To the contrary, many U.S. Big Tech companies view themselves primarily as global corporations, beholden to a constituency outside the United States and dedicated to its growth.[6] For example, more than 90 percent of Facebook's monthly users are now outside the United States and Canada.[7] In 2021, more than half of the revenue of Google's parent company, Alphabet, came from outside of the United States,[8] and as of July 2022, Google accounted for the majority of the global search engine market, controlling almost 94 percent of the market in India, 89 percent in Brazil, and over 80 percent of desktop search traffic in Hong Kong, Italy, and Spain.[9] The dominant global market share of Big Tech companies creates many economic advantages for the United States, but it also results in incentives to curry favor with U.S. adversaries and gain access to their consumer markets. Nowhere is this incentive stronger than it is with respect to China and its 1.4 billion consumers.

To cement and maintain this global reach, these companies often obey the local laws of such nations while openly flouting or selectively complying with U.S. government law enforcement or national security–related requests. Apple's 2016 defiance of the FBI after the 2015 San Bernadino Islamist terrorist attacks, its refusal to provide "substantive assistance" to the Justice Department after the 2019 Islamist terrorist attack in Pensacola, Florida, and Google's outright refusal to continue its contract with the Pentagon on Project Maven in 2018 are prime examples of this fitful cooperation with U.S. national security imperatives.[10]

At the same time, Big Tech companies actively contribute to the national security aims of adversary nations like China through joint technological development initiatives that are the CCP's price for manufacturing in China and enjoying access to the Chinese consumer market.[11]

- In 2016, Apple reportedly entered into an approximately $275 billion agreement with the Chinese party-state to develop China's "technological prowess" and economy.[12]

- Amazon maintains joint Amazon Web Services (AWS) "innovation centers" with the Chinese government throughout China, as well as Chinese government–linked data centers, and even partnered with a CCP propaganda arm as of at least 2018.[13]

- Google aids Chinese artificial intelligence (AI) development through a university with direct ties to the Chinese military and opened an AI research lab linked to the People's Liberation Army in Beijing in 2017.[14]

"National" champions these U.S. companies are not.

New entrants, not Big Tech monopolies, will produce the innovation America needs to stay competitive. A handful of Big Tech giants dominate U.S. digital markets today. These companies advertise their sizeable research and development (R&D) budgets: Google's parent company Alphabet, for example, spent more than $31 billion on R&D in 2021.[15] Their market position as monopolists, however, makes them less likely to innovate.

This phenomenon is not new. As long ago as 1962, economist Kenneth Arrow explained that an incumbent company's incentive to innovate is lessened because any innovation would replace existing sales.[16] To take a concrete example, AT&T, the dominant mid–20th century telecommunications company, funded an enormous amount of research at Bell Laboratories. Yet when a Bell Labs engineer developed magnetic tape and built the first telephone answering machine in the 1930s, AT&T's management suppressed the innovation for more than 20 years out of fear that answering machines would lead to fewer telephone calls.[17] In a similar vein, Google's R&D budget is not guaranteed to lead to innovation, and even if it does, the innovation is likely to be in areas of commercial interest to Google like search engine algorithms, not necessarily in areas of importance to national security.

Even in areas like AI where Google's research may be helpful to national security, new market entrants like Anduril, Shield AI, SpaceX, Palantir, Rebellion Defense, and others are genuine national security innovators.

From autonomous systems to robotics to all-domain command and control systems, these start-ups are coupling dynamism with an explicit desire to solve America's national security issues.[18] For example:

- Shield AI's "Hivemind" was the first autonomous AI pilot deployed since 2018, intended to enable autonomous drone swarms and aircraft that do not require GPS, communications, or even a human aviator.[19] Moreover, unlike entrenched Big Tech companies, part of Shield AI's stated mission is to "advance U.S. core values."[20]

- New entrant Anduril's autonomous underwater vehicles and AI-driven software and hardware layering systems led to multiple government contracts, including one worth almost $1 billion in 2022, and a valuation nearing at least $7 billion.[21] At a July 2022 conference, Palmer Luckey, Anduril's founder and former Facebook employee, reportedly noted that his former company and other Big Tech platforms use their resources and world-class talent primarily to build "tech toys and social apps" instead of committing to more serious U.S. national security applications.[22]

- Venture Capital firm A16z's Katherine Boyle identifies what is required to fix problems like those in national security: "serious founders...willing to build something new from nothing."[23]

Not long ago, Google, Facebook, and Apple were themselves small, innovative start-ups. Vigorous competition from new market entrants, not the R&D budgets of a handful of Big Tech monopolies, will be the key to U.S. success against the threat from China.

By contrast, Big Tech firms seek to entrench their monopolies by erecting high barriers to entry, engaging in rampant self-preferencing and other anti-competitive practices, and buying and killing innovative young companies.[24] Common behavior includes Apple's penchant for "Sherlocking," or stealing the core functions of the third-party applications it hosts, and demanding 30 percent commissions on in-app purchases from smaller companies.[25] Amazon effectively requires smaller companies to give it the right to buy massive stakes in those companies for extremely deep discounts rather than at market value.[26] Big Tech companies also hoard talent by hiring programmers to "work on next to nothing," in the words of venture capitalist Chamath Palihapitiya, solely to prevent them from being hired by other companies where their skillsets could disrupt the incumbent's business.[27]

Similarly, Big Tech companies are no strangers to the practice of "killer acquisitions," or buying out innovative young businesses just to kill them so they cannot compete with the acquirer in the future.[28] As part of this strategy, Big Tech companies specifically target and terminate the smaller company's innovation initiatives in order to strangle the future competitor and its incipient ideas in the crib.[29]

America cannot count on Big Tech to help fight China when Big Tech allies with China. Despite the national security threat from Communist China, some Silicon Valley companies were built through partnerships with the CCP that are now difficult for them to dissolve. Apple, for instance, assembles nearly every iPhone, iPad, and Mac computer it produces in China. The country is Apple's second-largest consumer market, with sales there making up nearly a fifth of the company's annual revenue.[30]

Apple's dependence on Chinese engineering, manufacturing, and consumers leaves the company at the mercy of CCP demands. In 2017, for example, the company agreed to move the sensitive personal information of Chinese users of its iCloud service—including text messages, emails, photos, and personal contacts—to servers inside China along with the encryption keys for that personal information.[31] On those servers, the iCloud data are owned not by Apple but by a Chinese state-owned company that has the legal authority to cooperate with Chinese security services.[32]

As the strategic competition between the United States and China has intensified, Apple has doubled down on its ties with China. In developing its new iPhone 14, Apple decided to add memory chips from Yangtze Memory Technologies (YMTC) to its supply chain, choosing YMTC over suppliers in South Korea.[33] The Chinese government owns 24 percent of YMTC, and congressional leaders have noted that there is credible evidence that the company violates U.S. export control laws by selling goods to Huawei.[34] Apple also recently ordered its Taiwan-based suppliers to label their products as made in either "Taiwan, China" or "Chinese Taipei," blocked the Voice of America mobile app from its App Store in China, and shifted significant portions of its design and engineering work from the United States to China.[35] Time and again, Apple has chosen to deepen its partnership with China, giving the CCP increased leverage over the company.

Although other Big Tech companies are less dependent on China than Apple, most have few qualms about helping the CCP to preserve their access to the Chinese market. Amazon Web Services, for instance, operates at least five joint operations centers in China. At those centers, technology incubators assist companies that participate in the Chinese military–civil fusion program and work with companies that enable electronic surveillance of ethnic Uighurs in China's Xinjiang province.[36]

And Amazon is not alone. Artificial intelligence may prove to be one of the key battlegrounds of competition between the United States and China, yet 10 percent of the collective AI research labs of Facebook, Google, IBM, and Microsoft were based in China at the end of 2020.[37] Microsoft has also announced a collaborative AI initiative with ByteDance, the Chinese parent company of TikTok.[38]

When still in government, Chairman of the Joint Chiefs of Staff General Joseph Dunford explained that Google's AI research in China "indirectly benefits the Chinese military and creates a challenge for us in maintaining a competitive advantage."[39] Similarly, between 2006 and 2010, Google's search engine censored results in China at the behest of the CCP.[40] In 2018, the company then attempted to build a Chinese censorship-compliant search engine until a public backlash caused it to drop the project.[41] That same year, Google refused to bid on Defense Department contracts for cloud computing, claiming that the work would conflict with its AI principles.[42] Google has since relaxed its prohibition on working with the U.S. military, but their past actions make clear that Big Tech companies should not be counted as American "national champions" against the threat from China.

Big Tech's National Security Arguments Fall Flat

Big Tech's campaign of open letters and op-eds from former national security officials relies on a mix of irrelevant or weak arguments that the legislative and executive branches should reject when considering potential antitrust reforms. According to *Politico*, all 12 former national security officials who signed a September 2021 letter warning against the antitrust bills on national security grounds have ties to Big Tech.[43] Because AICOA and the Open App Markets Act have gained momentum in the Senate, the arguments from Big Tech's lobbyists and other paid influencers focus on the provisions of those bills, but the same arguments would apply (and should be rejected) for any similar legislation or regulatory measures.

Interoperability and non-discrimination are not national security threats. One Big Tech argument is that antitrust reforms will force platforms to lower their defenses against threats from hostile states like China and Russia. By requiring U.S. tech platforms to include interoperability features that allow users to switch easily from one platform to another and mandating that they provide non-discriminatory access to competitors, Big Tech argues, the antitrust reforms will "result in major cyber threats, misinformation, access to data of U.S. persons, and intellectual property theft."[44]

This argument, however, ignores the text of both AICOA and the Open App Markets Act, which only prohibit Big Tech companies from taking actions that discriminate against competitors or give a preference to their own products.[45] Security and privacy enhancements that apply equally to all users of a platform or a service—including to competitors—would not run afoul of the bills' prohibitions.

This Big Tech argument also ignores provisions in both bills that allow tech companies to keep hostile actors off their platforms, even if the hostile actors may come in the guise of competitors. AICOA, for instance, expressly excludes any entity controlled by the Chinese government or any other foreign adversary from its protections and states that nothing in the bill shall require a tech company to share data with an entity that is sanctioned or determined to be a national security risk by the U.S. government.[46] These broadly worded exceptions will require refinement by courts and regulatory agencies to ensure that they are applied fairly and effectively, but Big Tech's national security alarmists ignore the exceptions altogether in the hope of bogging down the debate in misdirection.

Even without legislative exceptions, Big Tech's security and privacy arguments carry little weight on their own merits. For example, Apple has long forced iPhone users to download new apps through the company's own App Store—where Apple imposes a 30 percent fee on in-app purchases—and no other means. Users are unable to avoid Apple's fees by accessing competing app stores or "side-loading" apps directly to their phones. Google, by comparison, allows side-loading on Android mobile phones but does not allow competing app stores.

Apple claims that the Open App Markets Act's requirement that the company allow the installation of "third party apps or app stores through means other than its app store" would open iPhone users to security risks, including state-sponsored attacks.[47] But allowing side-loading would not force users to engage in the practice. Rather, users would be free to choose Apple's App Store with its security moderation and in-app fees, a competing app store with different moderation practices and different fees, or no app store at all.

Even with its monopoly, Apple is unable to screen apps for security risks effectively: Numerous iPhone apps, including apps that athletes at the 2022 Beijing Winter Olympics were forced to download, are riddled with Chinese surveillance tools.[48] If Apple allowed competing app stores, those app stores could be policed by antivirus and cybersecurity firms that might screen security risks just as well as or even better than Apple does.[49] Moreover, in direct contravention of its own security arguments for maintaining the dominance of the App store, Apple still extols the security benefits of its Mac desktop and laptop computers—products that permit the installation of applications outside of the company's store.[50]

Contrary to Big Tech's claims, ending app store monopolies might even strengthen, not harm, national security. Using its app store monopoly, Apple blocks users in China from downloading Virtual Private Network (VPN) applications, encrypted messaging applications such as Signal, and apps from independent media outlets.[51] As a result, Chinese citizens are unable to access information and communications tools that would allow them to evade ubiquitous government surveillance and censorship. Despite Apple's claim that the Open App Markets Act would harm national security, Chinese dissidents might appreciate the option to side-load VPN apps or even to use app stores that do not appease the CCP.

This is not the first time that Big Tech companies have attempted to use security concerns as a pretext for anticompetitive conduct.[52] Despite Apple's arguments that its app store restrictions were necessary to safeguard user privacy and cybersecurity, a September 2021 opinion in *Epic Games Inc. v. Apple Inc*. found that the company's concerns did not shield it from liability under California law for its anti-steering behavior, even as the court considered and rejected Epic's other antitrust claims.[53]

In short, national security and robust competition are not mutually exclusive. Antitrust reforms can and should be crafted to avoid requiring the potential transfer or sharing of data with the People's Republic of China or "the government of another foreign adversary," and fair competition does not preclude tech platforms from enhancing their own security as needed.[54] As Harvard cybersecurity scholar Bruce Schneier details in his 2022 letter supporting AICOA and the Open App Markets Act, "Any future changes that a platform makes to enhance privacy and security will still be permitted, as long as those changes are applied fairly to the platform's own products and services as well as to third parties."[55]

Numerous legislative and regulatory actions are available to mitigate national security threats. Even if, for the sake of argument, antitrust reforms had the incidental effect of complicating security efforts by Big Tech platforms, a wide variety of other actions could help to mitigate cybersecurity and supply chain threats to national security. Mobile apps like TikTok present a real and significant threat to Americans' privacy and security, even without antitrust enforcement against Apple and Google's app stores.

For example, TikTok logs all of its users' keystrokes and screen taps, including on third-party websites accessed through the app, and Chinese employees of its parent company, ByteDance, can access data of American users.[56] Despite numerous concerns about possible Chinese government access to sensitive personal data, the Biden Administration has yet to take action against TikTok, preferring instead to rescind President Donald Trump's ban without implementing any measures to mitigate the app's

threat to national security.[57] TikTok is also available through both Apple's App Store and the Google Play store for Android phones, raising doubt about both companies' claims that their app store monopolies lead to improved user privacy and security.

Similarly, existing executive branch authorities could be used to counter Chinese and Russian threats to cybersecurity and data privacy. To date, the Biden Administration has lacked the will to use these authorities. In May 2019, President Trump issued an executive order that empowered the Department of Commerce to block transactions involving information and communication technology and services (ICTS) from a foreign adversary that threatened national security.[58] That order was renewed but modified in June 2021 by President Joseph Biden, who added "connected software applications" to the scope of the Commerce Department's review authority.[59]

To implement either order, the Biden Administration must finalize implementing regulations. Nearly a year after making its proposal, the Commerce Department has yet to issue a final rule on ICTS transactions.[60] To the extent that Big Tech companies genuinely fear that antitrust reforms may embolden nation-state cybersecurity threats against American users, those threats will be mitigated most effectively by robust review of ICTS transactions involving Chinese and Russian software companies.

What Congress and the Administration Should Do

As noted, there are several legislative and regulatory actions that can be taken to counter Chinese and Russian threats to U.S. cybersecurity and data privacy. Specifically, Congress should:

- **Reform and modernize** U.S. antitrust laws based on competition principles and not specious national security arguments.
- **Expand** prohibitions on investments in Chinese military-related and surveillance-related companies to include outbound investment and partnerships.
- **Impose** transparency requirements for U.S. companies that operate in China.
- **Prohibit** joint ventures and R&D partnerships with Chinese state-owned entities.

The Department of Justice should:

- **Determine** whether Big Tech companies, almost all of which operate in countries all over the world (including countries with endemic corruption), are in strict compliance with the Foreign Corrupt Practices Act.[61]

- **Restore** its China Initiative to elevate the priority of investigations and prosecutions of Chinese covert political influence and economic espionage.[62]

The Department of Commerce should:

- **Fulfill** its responsibilities under the June 2021 executive order to recommend actions to mitigate national security threats from Chinese tech companies.

- **Finalize** its proposed regulation under President Trump's and President Biden's ICTS executive orders.

Conclusion

When considering antitrust reforms, Congress and the executive branch should look past Big Tech's self-serving national security arguments. Global companies like Google, Apple, and Amazon are not "national champions" like China's state-sponsored tech companies, not least because they are entangled with the CCP. U.S. national security will be advanced by encouraging innovation from new competitors that place American values first.

Moreover, many of the legislative reforms under consideration have been designed specifically to mitigate any national security concerns, and other policy tools can be employed to counter threats to cybersecurity and data privacy from adversaries like China and Russia. Policymakers should reject specious Big Tech–funded national security appeals and instead consider antirust reforms on their merits.

Michael J. Ellis is Visiting Fellow for Law and Technology in the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation. Mr. Ellis also serves as General Counsel of Rumble Inc., a company engaged in ongoing antitrust litigation against Google. **Kara Frederick** is Director of the Technology Policy Center at The Heritage Foundation.

Endnotes

1. S. 2992, American Innovation and Choice Online Act, 117th Cong., introduced October 18, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2992 (accessed October 18, 2022).
2. S. 2710, Open App Markets Act, 117th Cong., introduced October 11, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/2710 (accessed October 18, 2022).
3. Letter from Peter Hyun, Acting Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice, to The Honorable Richard J. Durbin, Chairman, Committee on the Judiciary, U.S. Senate; The Honorable Amy Klobuchar, Chairwoman, Subcommittee on Competition Policy, Antitrust, and Consumer Rights, Committee on the Judiciary, U.S. Senate; The Honorable Charles E. Grassley, Ranking Member, Committee on the Judiciary, U.S. Senate; and The Honorable Mike Lee, Ranking Member, Subcommittee on Competition Policy, Antitrust, and Consumer Rights, Committee on the Judiciary, U.S. Senate, supporting S. 2992 and H.R. 3816, March 23, 2022, https://www.justice.gov/ola/page/file/1488741/download (accessed October 17, 2022).
4. James R. Clapper, former Director of National Intelligence; Jane Harman, former U.S. Representative from California, former Ranking Member, House Intelligence Committee; Jeh C. Johnson, former Secretary of Homeland Security; Michael J. Morell, former Acting Director and Deputy Director, Central Intelligence Agency; Leon E. Panetta, former Secretary of Defense, former Director, Central Intelligence Agency; Admiral Michael S. Rogers, former Commander, U.S. Cyber Command, former Director, National Security Agency; and Frances F. Townsend, former Assistant to the President for Counterterrorism and Homeland Security, "Open Letter from Former Defense, Intelligence, Homeland Security, and Cyber Officials Calling for National Security Review of Congressional Tech Legislation," April 18, 2022, https://docs.house.gov/meetings/JU/JU00/20220728/114924/HHRG-117-JU00-20220728-SD008.pdf (accessed October 17, 2022); Letter from Robert Cardillo, former Director, National Geospatial-Intelligence Agency; Dan Coats, former Director of National Intelligence, former U.S. Senator from Indiana; Admiral James Foggo III, former Commander of U.S. Naval Forces Europe–Africa, Distinguished Fellow, Council on Competitiveness; Richard H. Ledgett Jr., former Deputy Director, National Security Agency; Susan M. Gordon, former Principal Deputy Director of National Intelligence; Michael Morell, former Acting Director and Deputy Director, Central Intelligence Agency; John D. Negroponte, former Deputy Secretary of State, former Director of National Intelligence; Leon E. Panetta, former Secretary of Defense, former Director, Central Intelligence Agency; Vice Admiral Jan E. Tighe, former Director of Naval Intelligence, former Commander of the Tenth Fleet; Frances Townsend, former Assistant to the President for Counterterrorism and Homeland Security; Dr. Michael Vickers, former Undersecretary of Defense for Intelligence; and Admiral James "Sandy" Winfield Jr., former Vice Chairman of the Joint Chiefs of Staff, letter to The Honorable Nancy Pelosi, Speaker of the House, and The Honorable Kevin O. McCarthy, House Minority Leader, September 15, 2021, https://www.axios.com/2021/09/15/china-antitrust-big-tech-national-security (accessed October 17, 2022). Cited hereafter as Clapper et al. letter, April 18, 2022, and Cardillo et al. letter, September 15, 2021.
5. Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emergency Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental (DIUx), January 2018, https://nationalsecurity.gmu.edu/wp-content/uploads/2020/02/DIUX-China-Tech-Transfer-Study-Selected-Readings.pdf (accessed October 17, 2022).
6. Mark Zuckerberg, "Understanding, Facebook's Business Model," Meta, January 24, 2019, https://about.fb.com/news/2019/01/understanding-facebooks-business-model/ (accessed October 11, 2022); Sarah Frier, "Facebook Reaps $1 Trillion Reward for Grow-at-Any-Cost Culture," Bloomberg, July 1, 2021, https://www.bloomberg.com/news/articles/2021-07-01/facebook-fb-reaps-1-trillion-reward-for-grow-at-any-cost-culture (accessed October 17, 2022).; Statista, "Meta's Global Revenue as of 2nd Quarter 2022," July 28, 2022, https://www.statista.com/statistics/422035/facebooks-quarterly-global-revenue/ (accessed October 17, 2022).
7. Justin Scheck, Newley Purnell, and Jeff Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show," *The Wall Street Journal,* September 16, 2021, https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers-response-is-weak-documents-11631812953 (accessed October 17, 2022).
8. Alphabet Inc., Form 10-K for the Fiscal Year Ended December 31, 2021, U.S. Securities and Exchange Commission, February 1, 2022, goog-20211231 (sec.gov) (accessed October 17, 2022).
9. Statista, "Share of Desktop Search Traffic Originating from Google in Selected Countries as of July 2022," https://www.statista.com/statistics/220534/googles-share-of-search-market-in-selected-countries/ (accessed October 17, 2022).
10. When it comes to policing the speech of Americans, U.S. Big Tech companies appear to be more willing to comply with government requests for censorship than they are when presented with bona fide national security requests. Compare Alex Berenson, "The White House Privately Demanded Twitter Ban Me Months Before the Company Did So," Unreported Truths, August 12, 2022, https://alexberenson.substack.com/p/the-white-house-privately-demanded (accessed October 17, 2022) with Tim Cook, "A Message to Our Customers," Apple Inc., February 16, 2016, https://www.apple.com/customer-letter/ (accessed October 17, 2022), and Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *The New York Times*, June 1, 2018, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html (accessed October 17, 2022).
11. National Intelligence Law of the People's Republic, Adopted at the 28th Meeting of the Standing Committee of the 12th National People's Congress, June 27, 2017, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (accessed October 17, 2022).
12. Wayne Ma, "Inside Tim Cook's Secret $275 Billion Deal with Chinese Authorities," *The Information*, December 7, 2021, https://www.theinformation.com/articles/facing-hostile-chinese-authorities-apple-ceo-signed-275-billion-deal-with-them (accessed October 17, 2022).

13. Nathan Picarsic and Emily de La Bruyère, *Corporate Complicity Scorecard: An Assessment of U.S. Companies' Exposure to Military Modernization, Surveillance, and Human Rights Violations in the People's Republic of China*, Victims of Communism Memorial Foundation and Horizon Advisory, published February 2022, https://victimsofcommunism.org/wp-content/uploads/2022/02/Corporate-Complicity-Scorecard-2.3.22.pdf (accessed October 17, 2022); Steve Stecklow and Jeffrey Dastin, "Special Report: Amazon Partnered with Chinese Propaganda Arm," Reuters, December 17, 2021, https://www.reuters.com/world/china/amazon-partnered-with-china-propaganda-arm-win-beijings-favor-document-shows-2021-12-17/ (accessed October 17, 2022).
14. Nathan Su, "Google Works on AI with Top Chinese University That Has Ties to China's Military," *The Epoch Times*, July 26, 2019, https://www.theepochtimes.com/google-works-on-ai-with-top-chinese-university-that-has-ties-with-chinese-military_3012365.html (accessed October 17, 2022); Ariel Zilber, "'A.I. Is a Military Technology': Silicon Valley Visionary Peter Thiel Ramps up His Attack on Google for Conducting Artificial Intelligence Research in China that Can Be Seized by Beijing While Refusing to Do Business with the US Military in Scathing Op-Ed," *Daily Mail*, August 2, 2019, https://www.dailymail.co.uk/news/article-7314519/Peter-Thiel-slams-Google-carrying-artificial-intelligence-research-China.html (accessed October 17, 2022).
15. Alphabet Inc., Form 10-K for the Fiscal Year Ended December 31, 2021.
16. Kenneth J. Arrow, "Economic Welfare and the Allocation of Resources for Invention," in National Bureau of Economic Research, *The Rate and Direction of Economic Activity: Economic and Social Factors* (Princeton, NJ: Princeton University Press, 1962, pp. 609–626, https://www.nber.org/system/files/chapters/c2144/c2144.pdf (accessed October 17, 2022).
17. Mark Clark, "Suppressing Innovation: Bell Laboratories and Magnetic Recording," *Technology and Culture*, Vol. 34, No. 3 (July 1993), pp. 516–538, https://www.jstor.org/stable/3106703 (accessed October 17, 2022).
18. Mark Sullivan, "Palmer Luckey: The U.S. Is Falling Behind in Defense Because Big Tech Is Scared of China," *Fast Company*, July 14, 2022, https://www.fastcompany.com/90769130/palmer-luckey-big-tech-defense-china (accessed October 17, 2022).
19. Shield AI, "The World's Best AI Pilot: Hivemind," https://shield.ai/hivemind/ (accessed October 17, 2022).
20. Ibid.; press release, "Shield AI Awarded Max AFWERX STRATFI Contract Focused on Operational Intelligent," Shield AI, January 27, 2022, https://shield.ai/shield-ai-awarded-max-afwerx-stratfi-contract-focused-on-operational-intelligent/ (accessed October 17, 2022).
21. Andrew Eversden, "Anduril Nets Biggest DoD Contract to Date: Signifier or Outlier for Defense Start-Ups?" *Breaking Defense*, January 24, 2022, https://breakingdefense.com/2022/01/anduril-nets-biggest-dod-contract-to-date-signifier-or-outlier-for-defense-start-ups/ (accessed October 17, 2022); Ingrid Lunden. "Anduril Is Raising up to $1.2 Billion, Sources Say at a $7 Billion Pre-Money Valuation, for Its Defense Tech," *TechCrunch*, May 24, 2022, https://techcrunch.com/2022/05/24/filing-anduril-is-raising-up-to-1-2b-sources-say-at-a-7b-pre-money-valuation-for-its-defense-tech/ (accessed October 17, 2022).
22. Sullivan, "Palmer Luckey: The U.S. Is Falling Behind in Defense Because Big Tech Is Scared of China"; *Fortune* on Demand, "Brainstorm Tech 2022: What Keeps Palmer Luckey up at Night," updated July 18, 2022, https://fortune.com/videos/watch/Brainstorm-Tech-2022-What-Keeps-Palmer-Luckey-Up-At-Night/761cc599-e940-4485-988d-a85d99efe553 (accessed October 17, 2022).
23. Katherine Boyle, "The Case for American Seriousness," *Common Sense*, April 18, 2022, https://www.commonsense.news/p/the-case-for-american-seriousness (accessed October 17, 2022).
24. Colleen Cunningham, Florian Ederer, and Song Ma, "Killer Acquisitions," *Journal of Political Economy*, Vol. 129, No. 3 (March 2021), pp. 649–702, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3241707 (accessed October 11, 2022); Will Oremus, "The Time Jeff Bezos Went Thermonuclear on Diapers.com," *Slate*, October 10, 2013, https://slate.com/technology/2013/10/amazon-book-how-jeff-bezos-went-thermonuclear-on-diapers-com.html (accessed October 17, 2022); Richard Waters, "Big Tech's 'Buy and Kill' Tactics Come Under Scrutiny," *Financial Times*, February 13, 2020, https://www.ft.com/content/39b5c3a8-4e1a-11ea-95a0-43d18ec715f5 (accessed October 17, 2022).
25. Joel Thayer, "App Developers Are Caught in Big Tech's 'Squid Game,'" *Roll Call*, November 19, 2021, https://rollcall.com/2021/11/19/app-developers-are-caught-in-big-techs-squid-game/ (accessed October 17, 2022); Angela Chen, "Regulating or Breaking up Big Tech: An Antitrust Explainer," *MIT Technology Review*, June 5, 2019, https://www.technologyreview.com/2019/06/05/135080/big-tech-breakup-regulation-antitrust-apple-amazon-google-facebook-doj-ftc-policy/ (accessed October 17, 2022).
26. Dana Mattioli, "Amazon Demands One More Thing from Some Vendors: A Piece of Their company," *The Wall Street Journal*, June 29, 2021, https://www.wsj.com/articles/amazon-demands-one-more-thing-from-some-vendors-a-piece-of-their-company-11624968099?mod=trending_now_news_3 (accessed October 17, 2022).
27. Chamath Palihapitiya, "E64: Antitrust Standards and Enforcement, Tech Repricing, Lab Leak Obfuscation, E63 Reactions and More," All-In Podcast, 1:36:15 (35:09), January 22, 2022, https://www.youtube.com/watch?v=s9n9db373e8 (accessed October 17, 2022).
28. Gerrit De Vynck and Cat Zakrzewski, "Tech Giants Quietly Buy up Dozens of Companies a Year. Regulators Are Finally Noticing," *The Washington Post*, September 22, 2021, https://www.washingtonpost.com/technology/2021/09/20/secret-tech-acquisitions-ftc/ (accessed October 17, 2022).
29. Kim Hart, "Big Tech's Small Biz Squeeze," Axios, July 12, 2021, https://www.axios.com/2021/07/12/big-techs-small-biz-squeeze (accessed October 18, 2022).
30. Tripp Mickle and Yoko Kubota, "Tim Cook and Apple Bet Everything on China. Then Coronavirus Hit," *The Wall Street Journal*, updated March 3, 2020, https://www.wsj.com/articles/tim-cook-and-apple-bet-everything-on-china-then-coronavirus-hit-11583172087 (accessed October 18, 2022).

31. Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, "Censorship, Surveillance and Profits: A Hard Bargain for Apple in China," *The New York Times*, May 17, 2021, https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html (accessed October 18, 2022).
32. Ibid.
33. Jack Purcher, "China's Yangtze Memory Technologies Has Reportedly Entered Apple's iPhone 14 Supply Chain," Patently Apple Blog, September 7, 2022, https://www.patentlyapple.com/2022/09/chinas-yangtze-memory-technologies-has-reportedly-entered-apples-iphone-14-supply-chain.html (accessed October 198 2022).
34. Jack Purcher, "U.S. Lawmakers Warn Apple About the Use of Memory Chips from China's Yangtze Memory Technologies for the iPhone 14," Patently Apple Blog, September 9, 2022, https://www.patentlyapple.com/2022/09/us-lawmakers-warn-apple-about-the-use-of-memory-chips-from-chinas-yangtze-memory-technologies-for-the-iphone-14.html (accessed October 18, 2022).
35. Thomas Claburn, "Apple Tells Suppliers to Use 'Taiwan, China' or 'Chinese Taipei' to Appease Beijing," *The Register*, August 5, 2022, https://www.theregister.com/2022/08/05/apple_warns_suppliers_in_taiwan/ (accessed October 18, 2022); Brendan Carr (@BrendanCarrFCC, Twitter Post, April 21, 2022, https://twitter.com/BrendanCarrFCC/status/1517181456732540934?s=20 (accessed October 18, 2022); Tripp Mickle, "How China Has Added to Its Influence Over the iPhone," *The New York Times*, September 6, 2022, https://www.nytimes.com/2022/09/06/technology/china-apple-iphone.html (accessed October 18, 2022).
36. Michael Graham, "Amazon Entangled with Chinese Communist Surveillance State, Report Says," *Inside Sources*, April 21, 2021, https://insidesources.com/amazon-entangled-with-chinese-communist-surveillance-state-report-says/ (accessed October 18, 2022).
37. Klon Kitchen and Bill Drexel, "Pull US AI Research out of China," *Defense One*, updated August 11, 2021, https://www.defenseone.com/ideas/2021/08/pull-us-ai-research-out-china/184359/ (accessed October 18, 2022); Matt Sheehan, "Who Benefits from American AI Research in China?" MarcoPolo, October 21, 2019, 2022, https://macropolo.org/china-ai-research-resnet/?rp=e (accessed October 18, 2022).
38. Jonathan Vanian, "Microsoft and ByteDance Are Collaborating on a Big AI Project, even as US–China rivalry Heats up," CNBC, updated August 28, 2022, https://www.cnbc.com/2022/08/26/microsoft-tiktok-parent-bytedance-collaborate-on-ai-project-kuberay.html (accessed October 18, 2022).
39. Carla Babb, "Dunford: Google's Work with China 'Challenges' US Military Advantage," Voice of America, March 22, 2019, https://www.voanews.com/a/dunford-google-s-work-with-china-challenges-us-military-advantage/4842453.html (accessed October 17, 2022).
40. Matt Sheehan, "How Google Took on China—and Lost," *MIT Technology Review*, December 19, 2018, https://www.technologyreview.com/2018/12/19/138307/how-google-took-on-china-and-lost/ (accessed October 17, 2022).
41. Ibid; Editorial, "Google and Microsoft Must Explain Their Enabling of China's Genocide Propaganda," *Washington Examiner*, June 21, 2022, https://www.washingtonexaminer.com/opinion/editorials/google-microsoft-enabling-china-genocide-propaganda (accessed October 17, 2022).
42. Kate Conger and Daisuke Wakabayashi, "Google Executives Tell Employees It Can Compete for Pentagon Contracts Without Violating Its Principles," *The New York Times*, November 15, 2021, https://www.nytimes.com/2021/11/15/technology/google-ai-pentagon.html (accessed October 17, 2022).
43. Emily Birnbaum, "12 Former Security Officials Who Warned Against Antitrust Crackdown Have Tech Ties," *Politico*, September 22, 2021, https://www.politico.com/news/2021/09/22/former-security-officials-antitrust-tech-ties-513657 (accessed October 17, 2022); IAP [Internet Accountability Project], "Former Intel Officials' Tech Ties," September 2021, https://theiap.org/wp-content/uploads/2021/09/Big-Tech-Funding-Behind-National-Security-Official-Letter-on-Antitrust.pdf (accessed October 17, 2022); Cardillo et al. letter, September 15, 2021. Four of the signers of the September 15, 2021, letter (Leon Panetta, Richard Ledgett Jr., Michael Morell, and Michael Vickers) also signed the October 19, 2020, public statement mistaking Hunter Biden's emails for Russian disinformation. See Jim Clapper et al., "Public Statement on the Hunter Biden Emails," *Politico,* October 19, 2020, https://www.politico.com/f/?id=00000175-4393-d7aa-af77-579f9b330000 (accessed October 17, 2022).
44. Clapper et al. letter, April 18, 2022.
45. See S. 2992, § 3(a) (prohibiting, among other things, self-preferencing, limiting the ability of competitors to use a platform, and discriminatory application of terms of service "in a manner that would *materially harm competition*") (emphasis added); S. 2992, § 3(b)(2) (establishing an affirmative defense for other actions if the action "has not resulted in and would not result in material harm to competition"; and S. 2710, § 4 (establishing safe harbors for actions that improve privacy and security so long as the actions meet certain requirements, including that they are "not used as a pretext to exclude, or impose unnecessary or discriminatory terms" on competitors).
46. S. 2992, §§ 2(a)(2)(B)(ii) and 7(a)(iii).
47. S. 2710, § 3(d)(2); Reuters, "Apple Presses U.S. Lawmakers on Dangers of 'Sideloading' Apps Allowed by Bill," March 4, 2022, https://www.reuters.com/technology/apple-presses-us-lawmakers-dangers-sideloading-apps-allowed-by-bill-2022-03-04/ (accessed October 17, 2022).
48. Dustin Carmack, "Time to Call out China's Olympian Invasions of Privacy and Other Abuses," Heritage Foundation *Commentary*, February 4, 2022, https://www.heritage.org/asia/commentary/time-call-out-chinas-olympian-invasions-privacy-and-other-abuses.
49. Letter from Bruce Schneier to The Honorable Dick Durbin, Chair, Senate Judiciary Committee; The Honorable Amy Klobuchar, Chair, Subcommittee on Competition Policy, Antitrust, and Consumer Rights, Senate Judiciary Committee; The Honorable Chuck Grassley, Ranking Member, Senate Judiciary Committee; and The Honorable Mike Lee, Ranking Member, Subcommittee on Competition Policy, Antitrust, and Consumer Rights, Senate Judiciary Committee, "RE: S.2992 and S.2710," January 31, 2022, p. 3, https://www.documentcloud.org/documents/22084940-schneier-letter-to-senate-judiciary-re-app-stores-1 (accessed October 17, 2022). Cited hereafter as Schneier letter.

50. Ridge Policy Group, "Ridge, Napolitano, Others Send Letter to Congress Supporting Open App Markets Act," May 2, 2022, https://ridgepolicygroup.com/ridge-napolitano-others-send-letter-to-congress-supporting-open-app-markets-act/ (accessed October 17, 2022). The letter was signed by Tom Ridge, former Secretary of Homeland Security and former Governor of Pennsylvania; Janet Napolitano, former Secretary of Homeland Security and former Attorney General and Governor of Arizona; Pat Meehan, former Chairman of the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies; Steve Kohler, President of Ridge Global and former President of Winner Global Defense; and Amanda Gorton, CEO and Co-Founder of Corellium.
51. Cate Cadell, "Apple Says It Is Removing VPN Services from China App Store," Reuters, July 29, 2017, https://www.reuters.com/article/us-china-apple-vpn/apple-says-it-is-removing-vpn-services-from-china-app-store-idUSKBN1AE0BQ (accessed October 17, 2022); Katie Benner and Sui-Lee Wee, "Apple Removes New York Times Apps from Its Store in China," *The New York Times*, January 4, 2017, https://www.nytimes.com/2017/01/04/business/media/new-york-times-apps-apple-china.html (accessed October 17, 2022).
52. *Epic Games, Inc. v. Apple Inc.*, 559 F. Supp. 3d 898 (N.D. Cal. 2021), https://casetext.com/case/epic-games-inc-v-apple-inc-2 (accessed October 17, 2022).
53. Ibid., *passim*.
54. S. 2992, §§ 3(a)(8)(B), 3(c)(7)(A)(v), and 4(b).
55. Schneier letter, p. 3.
56. Felix Krause, "iOS Privacy: Announcing InAppBrowser.com—See what JavaScript Commands Get Injected Through an In-App Browser," Krause Fx, August 18, 2022, https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser (accessed October 17, 2022); David McCabe, "TikTok Tells Republican Senators How It Plans to Keep American Data away from China," *The New York Times*, July 1, 2022, https://www.nytimes.com/2022/07/01/technology/tiktok-tells-republican-senators-how-it-plans-to-keep-american-data-away-from-china.html (accessed October 17, 2022).
57. David McCabe, "How Frustration over TikTok Has Mounted in Washington," The New York Times, August 14, 2022, https://www.nytimes.com/2022/08/14/technology/tiktok-china-washington.html (accessed October 17, 2022). The Biden Administration is rumored to be considering additional executive action against TikTok. See, for example, Reed Albergotti, "Semafor Exclusive: Biden Will Crack Down on Chinese Tech with a New Executive Oder," *Semafor*, September 2, 2022, https://medium.com/semafor-media/semafor-exclusive-biden-will-crack-down-on-chinese-tech-with-a-new-executive-order-da466c263a8a (accessed October 17 2022).
58. Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019, in *Federal Register*, Vol. 84, No. 96 (May 17, 2019), pp. 22689–22692, https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf (accessed October 17, 2022).
59. Executive Order 14034, "Protecting Americans' Sensitive Data from Foreign Adversaries," June 9, 2021, in Vol. 86, No. 111 (June 11, 2021), pp. 31423–31426, https://www.govinfo.gov/content/pkg/FR-2021-06-11/pdf/2021-12506.pdf (accessed October 17, 2022).
60. U.S. Department of Commerce, "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications," Docket No. 211115, Notice of Proposed Rulemaking, *Federal Register*, Vol. 86, No. 225 (November 26, 2021), pp. 67379–67383, https://www.federalregister.gov/documents/2021/11/26/2021-25329/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software (accessed October 17, 2022).
61. Kara Frederick, "Combating Big Tech's Totalitarianism: A Road Map," Heritage Foundation *Backgrounder* No. 3678, February 7, 2022, https://www.heritage.org/technology/report/combating-big-techs-totalitarianism-road-map.
62. Michael J. Ellis, "DOJ Emboldens China by Ending Initiative Against Our Greatest Counterintelligence and Economic Espionage Threat," Heritage Foundation *Legal Memorandum* No. 297t, March 4, 2022, https://www.heritage.org/crime-and-justice/report/doj-emboldens-china-ending-initiative-against-our-greatest.