AMERICAN ECONOMIC LIBERTIES PROJECT

Big Tech Monopolies Endanger American Security

Big Tech companies fight regulation by claiming that they are a necessary force for American national security. Their record says otherwise.

June 2022

REPORT

AMERICAN ECONOMIC LIBERTIES PROJECT

economicliberties.us

INTRODUCTION

Large technology companies often claim that they are an essential bulwark of our national security, and that breaking them up or even regulating them would pose a major risk for our national security and digital privacy. During a congressional hearing in 2018 where he was grilled on data privacy abuse, Facebook CEO Mark Zuckerberg's notes included the line "US tech companies key asset for America; break up strengthens Chinese companies." One year later, Facebook COO Sheryl Sandberg repeated the line on CNBC, and former Google CEO Eric Schmidt echoed the same argument about his company, saying that regulating Google would hand China a competitive advantage in tech. Last year, a group of former defense and intelligence officials repeated their talking points, urging congress to not pass antitrust legislation. They left out that they all had financial ties to the Big Tech firms.

These claims, a transparent attempt to avoid regulation and antitrust action, rest on faulty assumptions: that big tech monopolies protect – rather than undermine – America's national security, that monopolies foster innovation instead of stifling it, and that Big Tech monopolies facilitate American security better than fair and competitive markets would. However, the recent behavior of these Big Tech monopolies shows that they routinely undermine American national security in service of their profit margins, and they aid in the technological and military innovations of foreign adversaries. Promoting them as "national champions" and shielding them from antitrust action is itself a threat to our national security.

When it conflicts with their durable profit margins and monopoly power, Google, Facebook, Amazon, Microsoft, and Apple have repeatedly endangered American national security interests to protect their bottom line. Big Tech monopolies have a consistent history of complying with and supporting the antidemocratic actions of authoritarian states like Russia and China, transferring important next-generation technological capabilities to overseas firms with deep ties to foreign governments and militaries. In many cases, these firms are either failing or refusing to protect the security of the United States and American citizens who use their services.

Here we show how Apple, Google, Facebook, Amazon, and Microsoft have repeatedly demonstrated that they are not here to strengthen U.S. national security or advance the public interest, but to maintain their monopolies over technology markets. Antitrust action against these firms is the best and only way to promote U.S. national security and safeguard U.S. sovereignty.

Apple

- In 2016, Apple CEO Tim Cook *caved* to Chinese government pressure and signed a secret $275bn deal that ensured Chinese regulators gave Apple special treatment. The deal committed Apple to using more Chinese technology in its products, sharing research with Chinese universities, and directly investing in Chinese tech firms to help them vanquish US competitors.

- Apple *has transferred* priceless technological knowledge to Luxshare and other Chinese firms, detailing how to build its products.

- In 2018, Apple *explicitly asked* creators of TV content on Apple TV not to criticize China. SVP of Internet Software and Services Eddy Cue told showrunners to "avoid portraying China in a poor light."

- Apple is currently *considering* awarding a computer memory chipmaking contract to Yangtze, a Chinese state-affiliated company playing what Beijing believes to be a critical role in its state-backed tech markets.

- Apple has *repeatedly refused* to allow law enforcement to access criminals' devices, inhibiting active investigations and making it more difficult for law enforcement to stop terrorist attacks and solve crimes.

- In September of 2021, Apple and Google *removed* a voting app created by the Russian political opposition leader after pressure from the Russian government.

- Apple's App Store is *lush with multimillion dollar scams* on its users, and the company is either uninterested or incompetent in stopping it. This undercuts the company's *loud protests* at the supposed "security risks" of allowing competition to its App Store.

- In 2020, Apple was *lobbying* on behalf of forced labor in China, attempting to weaken the Uyghur Forced Labor Prevention Act.

- In 2021, 7 Apple suppliers in China were *found* to have participated in labor programs suspected of using Uyghur forced labor, including Lens Technology, one of Apple's longest-running and highest-profile suppliers – which also supplies Amazon and Tesla.

- Apple Maps' inaccurate territorial distinctions has *imperiled* the safety of American citizens by sending them into Russian territory during the Ukraine War.

- In 2021, Apple *handed over* user data to hackers impersonating law enforcement officials who sent forged data requests.

Google

- In 2018, Google *abandoned* a contract to deliver the Pentagon drone AI technology, leaving the DOD with no alternative supplier.

- In 2017 to 2018, Google secretly worked with the Chinese government to *develop* a censored version of its search engine that would allow invasive surveillance of its citizens.

- Google is one of multiple Big Tech firms recruited to help the Chinese government build out its surveillance apparatus. A nonprofit led by Google and IBM executives *helped advance* the data-processing abilities of Semptian, a Chinese government-linked firm that serves the Chinese government's surveillance apparatus.

- In December 2017, Google *established* an "AI China Center," devoting several hundred engineers to the advancement of China's AI industry capacity mere months after Xi Jinping passed a resolution allowing him to remain in power for life.

- Fitbit, now acquired by Google, *facilitated* the location leaks of U.S. military personnel worldwide, including detailed information on their movements around military bases.

- In 2020, after being acquired by Google, defense industry contributor Boston Dynamics *backed out* of a Pentagon-backed tech collaborative alliance that worked on robotic solutions to military projects, setting the organization back years. Google sold Boston Dynamics to a foreign company in 2021.

- Google, along with Facebook, Apple, and other Big Tech firms, *have been giving sensitive personal information* to malicious actors who use it to advance sexual extortion schemes targeting women and minors.

Facebook

- Facebook *promoted and profited* from advertisements peddling illegal opioids, throughout the opioid epidemic. The ads remained on Facebook for months after an NBC News investigation, and weeks after U.S. officials declared opioid addiction a public health crisis.

- Facebook *regularly exposes minors* to active drug dealers, which has led youth drug deaths to soar from fentanyl-tainted pills that minors obtain through social media.

- Like Apple, Facebook *handed over* user data to hackers impersonating law enforcement officials who sent forged data requests.

- Multiple recent Facebook *data breaches* have released the vulnerable personal data of billions of users, including hundreds of millions of Americans. Americans' personal information has ended up on black markets to be resold for further criminal activity.

- Mark Zuckerberg has personally cozied up to Chinese authoritarianism for profit in numerous ways, including *writing a blurb* for Xi's book, *distributing Chinese state propaganda* to his employees, and even *asking* Xi to name his child.

- Facebook *developed censoring tools* to help the Chinese government curb free speech online.

- Despite extracting reams of personal and private data from users, Facebook has "no idea where all of its user data goes, or what it's doing with it," *according to* its own engineers.

- Facebook platforms organized crime, *including violent drug cartels* that utilize its applications as a marketing service, marketplace, and target-selecting database, all in one.

- Facebook *regularly helps* scammers impersonate U.S. soldiers, and does nothing to stop it.

- Facebook is a breeding ground for identity theft, *including* the identities of sitting U.S. Congressmembers. Identity theft scams on Facebook drain hundreds of millions of dollars from Americans' bank accounts yearly.

- Facebook far has *refused* a widespread takedown of Russian state accounts spreading misinformation about the war in Ukraine, *changing its policie*s based on convenience and flip-flopping on enforcement. Facebook also launched a political advocacy group that *exploited* the Russian invasion of Ukraine to parrot its parent company's anti-regulatory agenda.

- Facebook *enables* and profits from the harassment of victims of horrific shootings and other violent crimes, contributing to false claims that the events were staged.

Amazon

- Amazon *purchases* worker-surveillance cameras from Chinese companies complicit in human rights abuse.

- Amazon *operates* cloud technology centers in China that bring Amazon into direct contact with Chinese government, military, and surveillance entities, helping advance the Chinese military-civil fusion program.

- Even as Amazon CEO and former AWS chief Andy Jassy argues that the Chinese AI developments put U.S. tech innovation leadership at risk, Amazon *continues to hire* AI and machine-learning experts to work on "highly visible, high impact" projects for Chinese customers.

- Security experts have *linked* a rise in brazen robberies to the ease with which thieves have been able to resell stolen goods on Amazon and Facebook.

- Amazon has *actively facilitated* as much Chinese seller activity into the US as possible, spawning a wave of counterfeit and dangerous products. Meanwhile, the company *lobbies* against bills protecting customers from these counterfeit and unsafe products.

- Amazon has *promoted and profited from* the sale of malware devices that specifically target government officials with high clearance levels.

- Amazon's foray into low-orbit internet-providing satellite constellations has *raised concerns* among experts that inadequate safety features may damage the U.S. military's space presence.

Microsoft

- Microsoft's Beijing-based Research Asia Lab, the company's largest outside of the U.S., has been *credited* as "the single most important institution in the birth and growth of the Chinese AI ecosystem over the past two decades." After the lab produced the single most-cited paper in any academic field from 2014-2019, half the paper's researchers went on to work for a Chinese tech company *sanctioned* by the U.S. government for complicity in aiding Uyghur genocide. By 2021, *10 percent* of the collective AI research labs of Facebook, Google, IBM, and Microsoft was housed in China.

- Microsoft *has built* at least 10 data centers in China operated by a Chinese partner firm, meaning that Chinese state authorities have complete access to all data collected at the centers.

- Microsoft has *maintained* "strategic partner" status with a Chinese drone and imaging technology firm even after it was sanctioned by the U.S. government in 2020 for enabling wide-scale human rights abuses.

- Microsoft *lobbied* on behalf of China's Huawei, saying the U.S. government was treating it "unfairly" for designating the Chinese military-controlled telecom firm as a national security threat. Huawei was founded and run by a former Chinese army technologist.

AMERICAN ECONOMIC LIBERTIES PROJECT

The American Economic Liberties Project is a non-profit and non-partisan organization fighting against concentrated corporate power to secure economic liberty for all. We do not accept funding from corporations. Contributions from foundations and individuals pay for the work we do.

economicliberties.us

@econliberties

info@economicliberties.us