foreignpolicy.com /2020/06/22/zoom-china-us-cold-war-unsafe/

Silicon Valley Can't Be Neutral in the U.S.-China Cold War

Jacob Helberg

16-20 minutes

If there is a silver lining to the coronavirus, it is that Americans are finally alert to the threat that an ambitious, authoritarian China poses. Polling shows that the U.S. public has become significantly more hawkish on China since the crisis began; a bipartisan consensus is coalescing around the idea that the Chinese Communist Party's aims and values are incompatible with America's. Unfortunately, some of the United States' major tech companies are still trying to sit on an increasingly uncomfortable fence.

I know this issue well, because for several years I served as a policy advisor at Google. There, I learned that a company's policies, like a society's laws, reflect its most basic values. The problem today is that tech companies that are based in the United States but also operate in China are struggling to comply with values that are fundamentally at odds.

In the U.S. system, laws are legitimate insofar as they are conceived by what Jean-Jacques Rousseau called "the general will" of the people, expressed through the workings of a democratic political system. Laws that are arbitrary or imposed by the will of a single person of authority are illegitimate. Yet the Chinese system rests on the idea that the sole source of legitimacy is the CCP, which represents—it claims—the will of the Chinese nation in its entirety and violently suppresses challenges to its authority. This sharp tension between the political value systems that prevail in the two countries is a primary cause of the spiraling bilateral competition. Tech companies confront this tension when they are tasked to comply with Chinese laws, by enabling the arrest of dissidents for "subversion of state power" or the mass surveillance of Uighurs, which are rightly viewed by most Americans as immoral and illegitimate.

The natural response of most companies, which seek to maximize profits by operating in the world's two largest national markets simultaneously, is to straddle this divide. Think of this approach as "one company, two systems." I saw this well-intentioned strategy up close, through my brief exposure to Project Dragonfly, a since-shuttered effort to make a version of Google's search engine available behind China's so-called Great Firewall by conforming search results to CCP standards. The experience left me deeply convinced that the "one company, two systems" model does not work. Tailoring one's principles to make them compatible with the CCP's dictates makes them systemically incompatible with American values.

This contradiction was on display on June 3. Several hundred American and Chinese activists were commemorating the next day's 31st anniversary of the Tiananmen Square massacre when their Zoom videoconference cut out. The glitch, it turned out, was not technical but ideological. The same week, Zoom shut down the account of the California-based dissident Zhou Fengsuo. Elizabeth Economy, a prominent China scholar at the Council on Foreign Relations, then revealed that she, too, had been dropped from a Zoom seminar as she discussed Tiananmen Square, China's brutal oppression of its Uighur minority, and other taboo topics. "We all joked about it," she wrote, "but maybe there was no joke to be had." It certainly appears that the takedowns amounted to a CCP attempt at extraterritorial censorship—"no joke" indeed.

Zoom, a California-based videoconferencing company whose profile has soared during the coronavirus pandemic lockdowns, responded that the takedowns resulted only from the company's obligation "to comply with local laws"—China's laws, in this case. It apologized for impacting users outside of China, reinstated the accounts of U.S.-based activists, and pledged not to censor non-Chinese accounts.

Zoom also says that it is developing technology "to remove or block at the participant level based on geography." In other words, Zoom is rolling out a "one company, two systems" model—participants in China would be subject to censorship, but those outside of China would not.

> In other words, Zoom is rolling out a "one company, two systems" model—participants in China would be subject to censorship, but those outside of China would not.

> In other words, Zoom is rolling out a "one company, two systems" model—participants in China would be subject to censorship, but those outside of China would not.

The flaws in this model are already apparent. While Zoom assured users in the United States that they would not be penalized for violating Chinese speech restrictions, the company did not guarantee that it would not scan or monitor the conversations or accounts of U.S.-based users. Zoom also left unaddressed the question of what happens when a user in the United States converses across borders with a user in China—or when a Chinese citizen based in Vietnam uses Zoom for academic purposes and discusses the Tiananmen massacre in their native Mandarin.

In fact, Zoom can't offer meaningful reassurance on these issues. That's because the company, which employs at least 700 engineers in China through various subsidiaries, is subject to truly sweeping Chinese surveillance laws. Internet companies are under particular pressure from the authorities in China; huge amounts of labor are dedicated to making sure that content avoids crossing the government's lines. Zoom's own filings with the U.S. Securities and Exchange Commission acknowledge that its Chinese employees "could expose us to market scrutiny regarding the integrity of our solution or data security features." That's an understatement. The CCP so dominates Chinese-based technology companies that the Chinese app TikTok's algorithms privilege videos that praise President Xi Jinping and the Chinese government in deciding what to promote to the app's users in the United States. Similarly, each of Zoom's Chinese employees is subject to China's National Intelligence Law, which states that "any organization or citizen shall support, assist with, and collaborate with the state intelligence work in accordance with the law" and keep any assistance confidential.

In the United States, the relationship between private firms and the national security establishment is hardly flawless. But in general, Americans expect that companies will adhere to free expression, the rule of law, basic protections involving searches and seizures, and the requirements of due process. When excesses occur, they can be openly litigated and scrutinized by an uncensored press. In China, the primary expectation is total compliance with the CCP, without the slightest regard for privacy protections. Even the savviest attorneys will be hard-pressed to reconcile systems of laws that are inherently incompatible.

This isn't a hypothetical challenge. Zoom has admitted that the Chinese government asked it to terminate the activist accounts linked to the Tiananmen commemorations. So one has to ask: What else has the CCP asked Zoom to do that Zoom hasn't yet publicly admitted? Who's to say that the Chinese government—which has long engaged in aggressive economic espionage against American companies—hasn't tasked Zoom employees with monitoring sensitive business conversations for valuable insights? Or that a Chinese official hasn't threatened an engineer's family with legal jeopardy if the employee doesn't build a backdoor into Zoom's platform?

The magnitude of the problem that such security breaches would pose is hard to overstate.

> The magnitude of the problem that such security breaches would pose is hard to overstate.

The pandemic has been a jackpot for Zoom. Individuals and organizations have turned to the intuitive videoconferencing service to keep in touch with family, speed date, teach students, broadcast religious services, conduct business, and even hold cabinet meetings. In December 2019, Zoom had 10 million daily meeting participants. By April 2020, that number had spiked to 300 million. Due to security concerns, organizations such as SpaceX, NASA, Apple, and Google have banned employees from using Zoom for work purposes. The U.S. Senate, the Department of Defense, and the German government have similarly issued warnings and restrictions. But there's no avoiding the fact that an enormous amount of the world's interaction is occurring on a platform that, as the *New York Times*' Paul Mozur wrote, is caught "between the principles of free speech and the power of China's huge censorship machine." Back in March, I warned that Zoom was caught in an impossible position and might end up exposing its users. Unfortunately, it appears that this is exactly what transpired.

> The magnitude of the problem that such security breaches would pose is hard to overstate.

Zoom isn't alone in this conundrum. Apple—which manufactures its iPhones in China and sells more iPhones there than anywhere else—recently bowed to CCP requests to remove a popular podcast app from its App Store. Many tech firms, finding themselves caught between the imperatives of two very different systems, have either been forced out of China or simply chosen not to operate there at all. As companies such as Google, Netflix, Twitter, GitHub, and Facebook can all attest, the technical, legal, and moral challenges of serving users in the United States and China simultaneously are substantial.

Consider the technical challenges of operationalizing a "one company, two systems" model. Judging from the actions Zoom has taken, there are two principal ways the company could have built tools to allow it to comply with China's censorship laws relating to sensitive topics. Those tools either track and detect violating *accounts*, or they track and detect violating *content* (or some combination of both). Enforcing censorship laws by tracking violating *accounts* would require Zoom to collect and compile information on the *account owner* in order to determine the history and likelihood of that owner violating Chinese censorship laws. Enforcing these laws by tracking violating *content* would require Zoom to train a system, commonly referred to as a "classifier," that allows it to automatically scan ongoing conversations and decipher what is being shown and said. Even if Zoom develops a workable policy on such cases—a big "if," given the inherent ambiguities—any automated enforcement system is bound to encounter edge cases that will lead it to ensnare content it shouldn't. It is also unclear how it intends to continue complying with China's local laws and government requests if it fulfill its most recent promise of making end-to-end encryption available for all users globally.

Then there are the legal obstacles. Under international law, litigants can use the legal discovery process to compel a foreign corporation to produce information through its domestic affiliates, unless those affiliates have a substantially independent corporate governance structure. This means that if Zoom's subsidiaries in China are indeed controlled by Zoom, the Chinese government or any Chinese entity could compel the U.S.-based parent company to hand over information under the guise of a legal discovery request—assuming it chose not to use its authority to do so in secrecy under its National Intelligence Law. In theory, a U.S. district court might not enforce such a discovery request, but historically U.S. courts have ignored local "blocking" statutes to obtain the documents. These legal intricacies can prove sticky enough when the legal systems in question are those of two democracies that respect individual liberties and the rule of law. The difficulties grow immeasurably when one of the countries is a Leninist party-state.

There are also major ethical problems. It is becoming far harder for Silicon Valley idealists to reconcile—internally and externally—the conviction that their companies have company values with the idea that the products those companies make are value-agnostic. For instance, Christian media reported that Chinese Christians who joined a Sunday worship service via Zoom were later arrested by the CCP. How long will Zoom's American employees be content to cite compliance with "local laws" as their platforms are used to not only suppress free speech but also to enable the oppression of dissidents and minorities?

At Google, the answer was "not long." Many of the company's own employees turned against Project Dragonfly in an open letter to management.

Other firms could soon face similar quandaries. Amazon and Microsoft each operate cloud storage services in China. What would happen if the CCP pressured Microsoft to turn over information on a Chinese dissident if it wanted to keep operating in China? Ever since 2004, when Yahoo divulged to the Chinese government the email account of a newspaper editor named Shi Tao—who was subsequently sentenced to a decade of forced labor—this dilemma has haunted Silicon Valley. And what would happen if the CCP requested information on a user outside of China under the same conditions?

Finally, the most harmful weakness of "one company, two systems" is also the most overlooked: geopolitics.

> Finally, the most harmful weakness of "one company, two systems" is also the most overlooked: geopolitics.

Zoom's recent takedowns are likely to intensify a broader reckoning within the technology industry, which is being caused not by market pressures but by strategic pressures. The coronavirus pandemic has amplified and accelerated the thrum of a new cold war between an autocratic China and a democratic United States. That struggle features ambiguous gray-zone attacks that are both perpetual and strategically impactful, yet never quite meet conventional thresholds of war. It may well be decided by which country better harnesses the forces of technological innovation.

> Finally, the most harmful weakness of "one company, two systems" is also the most overlooked: geopolitics.

In this deepening conflict, major tech firms are essentially dual-use assets, in the sense that their civilian technologies can be repurposed as powerful weapons of asymmetric warfare. As Apple CEO Tim Cook remarked, "scraps of data … each one harmless enough on its own" can be aggregated and synthesized to derive and develop to algorithms that "know you better than you may know yourself." Different applications of dual-use technologies, from facial recognition to 5G networking, are already being weaponized as tools of political control and geopolitical influence by the Chinese state. As former

Democratic presidential candidate Pete Buttigieg summed it up, “China is using technology for the perfection of dictatorship.”

Governments are beginning to eye global technology companies as proxies—and potential targets—of their respective national power; politicians are talking about artificial intelligence the way they once spoke of the atomic bomb. Sooner or later, U.S. firms will find it untenable to remain neutral in this contest—let alone to accommodate autocrats in Beijing—while also retaining good relations with Washington. American policymakers will increasingly view U.S. companies that accommodate or assist the CCP as unpatriotic and corrosive to national security interests.

For many firms in Silicon Valley, this will be a rude shock. For years, major firms have been treated as quasi-sovereigns. Denmark appointed the world’s first official ambassador to the tech industry; Microsoft has proclaimed itself a “neutral digital Switzerland” and encouraged other companies to do the same. The perception is, as Palantir CEO Alex Karp wrote, “The U.S. Marine serves; the Silicon Valley executives walk.” Yet with Chinese tech titans, such as Huawei and Baidu, supporting the CCP’s revisionist agenda, American policymakers won’t have much tolerance for U.S. firms remaining nonaligned. The choice, as Republican Sen. Josh Hawley wrote earlier this month, is between “American principles and free-speech, or short-term global profits and censorship.” Hawley’s conclusion reflects the growing bipartisan mood among Washington policymakers and should be a wake-up call to the rest of us in Silicon Valley: “It is time for you to pick a side.”

Decoupling is increasingly accepted as the direction that trade policies are headed on both sides of the Pacific. With U.S.-China relations currently more volatile than at any time since Tiananmen, it is an open question whether this decoupling will be slow and soft or hard and fast. American companies should prepare for what was once unthinkable: a sudden, hard decoupling in technology verticals deemed vital to national security. Ultimately, Silicon Valley executives may not be interested in getting involved in a geopolitical contest, but the underlying divergent interests of the United States and China are rapidly ensuring this geopolitical contest is interested in Silicon Valley. Time is running short for firms to decide where they stand.