NEW AMERICA

November 2023

The Rise of Techno-Nationalism

Tianyu Fang & Tim Hwang

Open Technology Institute
Last edited on November 08, 2023 at 1:56 p.m. EST

About the Author(s)

Tianyu Fang is a MacArthur Tech and Democracy Fellow at New America.

Tim Hwang is a writer and researcher working on issues of science and technology policy.

About New America

We are dedicated to renewing the promise of America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

The Rise of Techno-Nationalism

Introduction

In the 2000s, U.S. foreign policy discourse adopted a specific vision of the internet and cutting-edge technologies at large that celebrated its potential as a lever for spreading free expression, democratic values, and trade globally. Over the past decade, this has shifted dramatically. Driven by increasing tensions with China and greater skepticism towards technology at home, the U.S. has adopted a foreign policy vision for technology that is increasingly anchored by national security concerns, focused on zero-sum competition, and less committed to openness.

This shift has emerged across multiple issue areas and in different communities. However, taken together, we believe they mark a major shift not only in the discourse around U.S. foreign policy, but also in thinking about domestic policy around technology and the technology industry. This paper aims to draw these disparate threads together and characterize them as part of a general trend in thinking that we dub "techno-nationalism."

This paper is broken into three parts. In Part I, we characterize the key tenets of techno-nationalism and discuss how it is distinct from policymaker thinking about technology that dominated during the 2000s. In Part II, we present two case studies, showing how techno-nationalist framings have shaped contemporary U.S. discussions around Chinese digital surveillance systems and the rise of TikTok. We also highlight how these viewpoints have often been at odds with technological realities and pushed towards harmful or partial policies. Finally, in Part III, we articulate a civil society agenda for building an alternative to the techno-nationalist position.

Part I: What Is Techno-Nationalism?

Techno-nationalism is a framework for U.S. foreign policy that has as its core tenets two main pillars. First, that geopolitical competition with China is both zero-sum and dependent on achieving technological superiority. And second, that national security and foreign policy considerations in the competition trump domestic considerations.

Pillar 1: Geopolitical competition is, at its root, a competition between distinct "Chinese" and "U.S." models of leveraging emerging technologies.

Techno-nationalism takes as a given that the most pressing issue facing U.S. foreign policy is the evolving geopolitical competition with China. It sees this competition as largely zero-sum, with the result being either the continued dominance of the United States over global affairs, or with China replacing the United States in this leading role over the coming decades.

Uniquely, techno-nationalism assumes that the pivotal arena in this competition will be a battle between different U.S. and Chinese models for developing and implementing cutting-edge technologies. These areas include artificial intelligence, semiconductors, social media, and biotechnology. These technologies are believed to provide a crucial edge not only to militaries in a potential conflict, but also in unlocking economic growth crucial to success.

In one example, the **Biden administration imposed a ban** in August on U.S. venture capital investment in China's key technology sectors. While the restrictions are intended to target military applications, they are part of a broader, targeted attempt to slow down China's quest for technological supremacy, following moves imposing export controls on advanced semiconductors earlier in 2022.

This position contrasts with a number of other alternatives. More dovish positions question the zero-sum nature of U.S.-Chinese technological competition, or whether the two nations are in competition at all. There are also variants in the more hawkish direction, as well. One might consider a path to victory for the United States in competition with China that emphasizes the need to conclusively outmaneuver China in international institutions and ally-building or to dominate in soft power.

Pillar 2: National security and foreign policy considerations are paramount in technology policymaking.

Techno-nationalism views the importance of the geopolitical conflict and national security considerations as paramount. Given the weight that techno-nationalism attributes to technology, it believes that policymaking around technologies should be driven by these considerations, rather than balanced against domestic considerations.

Substantively, this means that national security interests should outweigh demands by domestic constituencies for ensuring civil rights protection and public transparency. From an economic standpoint, it sees concerns around ensuring competitive markets in emerging technology and global free trade as taking a backseat to implementing policies in the interests of national security.

As we will later show in greater detail, while there are legitimate concerns about the social media platform TikTok, the attempted ban in Congress was a violation of open internet principles long heralded by U.S. technology activists and

policymakers—implicitly accepting that national security justifies stronger limitations on free competition in the market for social media.

This emphasis also has implications for "who is around the table" in the policymaking process. Techno-nationalists forward the notion of national security organizations and the intelligence community taking the leading, if not exclusive, role in technology policymaking. This is in contrast to a model that would advocate for greater public and civil society participation, or the leadership of agencies focused on trade and commerce.

The Techno-Nationalist Shift

Techno-nationalism has become a widespread framework for thinking about U.S. foreign policy, particularly in the context of competition with China. While echoes of techno-nationalist positions can always be identified historically, our contention is that it has come to replace the kind of U.S. foreign policy and technology that was ascendant during the early part of the twenty-first century. This earlier techno-optimist discourse emphasized themes that are in many ways quite the opposite of techno-nationalist positions, though equally concerned with advancing U.S. interests globally. Techno-optimists emphasized the potential of technologies—particularly the internet—as a tool for spreading democratic values and human rights, enabling global economic trade, and fostering dynamic competition across markets.

This was the internationalist vision once put forth by the U.S. government. "We need to work toward a world in which access to networks and information brings people closer together and expands the definition of the global community," **said then Secretary of State Hillary Clinton** in 2010. "Given the magnitude of the challenges we're facing, we need people around the world to pool their knowledge and creativity to help rebuild the global economy, to protect our environment, to defeat violent extremism, and build a future in which every human being can live up to and realize his or her God-given potential."

Our purpose in this paper is not to defend techno-optimism, which committed many errors on its own. However, we highlight this earlier period of discourse to emphasize how significant a change techno-nationalism has been to thinking about the intersection between technology and U.S. foreign policy.

This change has already begun to bring about significant changes in technology policymaking. In Part II, we examine two case studies to explore the practical impact of techno-nationalism and critique its impact.

Part II: Case Studies

Techno-nationalism is compelling in part because it presents a cohesive vision for how the United States must organize its domestic technological resources to

compete in the twenty-first century. This vision has shaped discourse, particularly around discussions of U.S.-Chinese competition, and is helping to give rise to a range of aligned policies that implement its ideas.

However, the trouble is that in many cases the techno-nationalist framing has been at odds with the facts, leading to policies that fail to address the broader ills being produced by emerging technology. This has been illustrated by two recent moments: one around China's digital surveillance systems, and another one around the rise of TikTok.

Social Credit and Digital Surveillance

In 2014, the Chinese State Council published a **six-year plan** to implement a nationwide social credit system. The plan, to be completed by 2020, entailed a broad range of endeavors to build safety and trust in economic and social functions by integrating information across databases, rewarding trustworthy behaviors, and penalizing untrustworthy conducts. One core mechanism of the guidelines is a blacklist for law enforcement that primarily targets corporations and entrepreneurs that violate industry regulations or fail to meet their legal obligations.

While no score-based program was mentioned in the 2014 plan, local experiments have caught much international attention. Since 2018, Chinese authorities have introduced pilot programs in 43 municipalities. The government of Rongcheng in the Shandong province **established a point-based system** to reward creditworthiness and punish untrustworthy conduct.

Techno-nationalist framings of these programs as an unprecedented and uniquely Chinese effort were pervasive in the media. *Foreign Policy* warned of the Communist Party's "massive experiment in ranking and monitoring Chinese citizens." The Australian Broadcasting Company described **the social credit system** as "a personal scorecard for each of China's 1.4 billion citizens." Beijing's "end-to-end grid of social control," according to the *Atlantic*, was intended to "**reach into every corner of existence** both online and off."

In 2018, former Vice President Mike Pence called the social credit score "an Orwellian system premised on controlling virtually every facet of human life." The **political theorist Francis Fukuyama** wrote that China's social credit system "combines all of the methods of artificial intelligence, big data, and pervasive sensors, and puts them in the hands of the Chinese state." Governor Ron DeSantis signed legislation that **banned "social credit scores"** in Florida against the "woke political ideology across the financial sector."

Specialists in Chinese law have **debunked** and **dismissed** such reports as **mischaracterizations**. In reality, the social credit system rarely affects ordinary citizens—their main targets were businesspeople in certain professional fields, such as government contractors, and punishable conduct was already subject to

existing forms of legal penalties. **Vincent Brussee argued** that China's social credit system, while far from benign, is "not the techno-dystopian nightmare we fear: it is lowly digitalized, highly fragmented, and primarily focuses on businesses." After the Chinese government **effectively outlawed score-based systems** as legal penalty, all pilot programs that overreached legal requirements —including Rongcheng—were either **discontinued or downscaled** as of 2021.

Moreover, the techno-nationalist frame inaccurately assumed that social credit programs were representative of a specifically Chinese vision of emerging technology. However, as Vincent Brussee demonstrates, China's own social credit system was made possible by ideas from U.S. and European corporations and governments. China's attempts to create a credit system trace back to the early 2000s and were in fact **inspired by U.S. credit reporting services** such as FICO, Dun & Bradstreet, and Standard & Poor's (now S&P). The design of China's credit system, in its early iteration, referenced U.S. legislations on credit management despite their later divergence in implementation. Commercial credit scores in China, such as Ant Financial's Sesame Credit, reflect financial creditworthiness in ways similar to U.S. and European credit bureaus.

Though credit bureaus do not incorporate political tendencies and ideological affiliations into their algorithms, they have historically **laid ground** for **discriminatory practices**. Credit bureaus are not government-owned, but their scoring models largely determine whether citizens qualify for basic services—from bank loans to job applications and apartment rentals. The introduction of data collection regimes has contributed to inequalities in access to financial and government services alike.

Despite exaggerated accounts of the social credit system, there is no denying that Beijing has adopted digital tools for oppression. Technologies such as digital surveillance, **facial recognition**, big-data analysis, and **predictive policing** have facilitated the Chinese government's **quest for stricter political control**, especially in its mass internment of Turkic Muslims in Xinjiang. The U.S. response to the Xinjiang crisis has focused on condemnations of the Chinese state. In 2020, Congress passed the **Uyghur Human Rights Policy Act** to impose sanctions on individuals and corporations.

But it is also true that Beijing's technology-enabled repression of ethnic minorities has global origins. In the wake of the September 11 attacks and heightened Islamophobia in North America and Europe, China became a willing participant in the U.S.-led war on terror, **adopting its tactics, languages, and discourse**. Chinese government and tech corporations have drawn on techniques from the expanded security apparatus in the West—including mass data analytics and government watch lists—that were justified in the name of counter-terrorism. "While the Chinese system is unique in terms of its scale and the depth of its cruelty," argued **anthropologists Darren Byler and Carolina**

Sanchez Boe, "terror capitalism is an American invention, and it has taken root around the world."

In the meantime, surveillance platforms similar to China's are increasingly influential in the United States. Palantir Technologies, for example, has worked in close collaboration with government agencies to adopt predictive policing mechanisms in **Los Angeles** and **New Orleans** through large-scale surveillance. Clearview AI, which offers facial recognition services to police officers, has **repeatedly violated privacy regulations** by collecting and selling faceprints en masse. While China-based firms such as SenseTime and Hikvision have rightfully been under public scrutiny, U.S. government contractors that develop similar policing technologies funded by U.S. taxpayers were largely left out of the discussion.

Again, techno-nationalist responses tend to highlight digital repression in Xinjiang as a phenomenon peculiar to the Chinese political system, insinuating that similar violations could not take place in liberal democracies. This wrongfoots the discussion from the very beginning, leading to policies that condemn harmful uses of the technology abroad while failing to recognize that the global origins of these uses emerge closer to home. A more nuanced view would recognize the ethical perils and social risks of surveillance systems at home and abroad, viewing paranoia about China's proposed programs in the broader framework of digital privacy and economic inequality.

TikTok

TikTok's connections to China has long raised concerns in Washington. There have been documented instances of China-based personnel accessing TikTok data, including one case in which ByteDance's Chinese employees **spied on U.S. journalists** covering the company. Critics argue that under China's data security and anti-espionage legislations, Chinese authorities can theoretically coerce ByteDance to turn over TikTok user data in the United States.

U.S. policymakers and tech leaders alike have adopted a techno-nationalist approach, framing the company as an agent of a foreign adversary. TikTok "is a tool that is ultimately within the control of the Chinese government, and to me, it screams out with national security concerns," **said FBI Director Christopher Wray**, who believed China to be "not just a whole-of-government threat, but a **whole-of-society threat**."

U.S. policymakers have responded to these risks by limiting access to TikTok. After the Committee on Foreign Investment in the United States **opened an investigation of ByteDance's acquisition** of Musical.ly in 2019, the Trump administration issued an executive order in August 2020 to effectively ban the app in the United States. While Trump's ban was challenged in court and eventually reversed by President Joe Biden, a series of federal and state legislations banned the use of TikTok on government devices. In March 2023,

TikTok CEO Shou Zi Chew testified before Congress as the Senate introduced a new bill to limit access to the popular short video platform, owned by the China-based ByteDance. The **RESTRICT Act**, if passed, would empower the executive branch to ban any technology from "foreign adversaries" deemed dangerous to national security; it also vows to penalize Americans who use digital tools to circumvent proposed restrictions.

The techno-nationalist response to TikTok's alleged threats is predicated upon two wrong assumptions. First, it identifies the problems of TikTok with its Chinese ownership, instead of failures of social media regulations across the board. This is consistent with a view that TikTok represents a specifically Chinese vision of how social media platforms should be architected.

This parallels the discussion around social credit: presenting a misleading vision of the technology and missing the many parallels that link TikTok with the broader field of social media companies. Without dismissing Beijing's ever-tightening grip on China's tech sector, we note that allegations of TikTok being under the Chinese government's control are often **hypothetical and unsubstantiated**. Members of Congress throughout the Chew hearing interrogated him on issues such as addiction, mental health, privacy, misinformation, and political influence. These threats do not come from the Chinese Communist Party; rather, they are concerning problems with other social media platforms, especially U.S.-based alternatives. If TikTok's practices do not deviate from industry norms, then these norms should warrant examination and regulation.

Second, comprehensive bans on foreign apps implicitly reject the open vision of the internet that both the U.S. government and civil society have historically sought to defend. This is consistent with the idea that national security should outweigh traditional commitments to ensuring open competition and free expression online. Ironically, attempts to limit access to services on grounds of foreign ownership **echo China's claim** to "cyber sovereignty," which views participation on the global internet as a threat to national security. This signals a convergence, not divergence, between U.S. and Chinese policy.

Rather than addressing concerns about algorithm-based social media platforms across the board, this techno-nationalist response leaves TikTok's U.S. competitors intact and views them as vehicles for boosting U.S. power in the new tech arms race. This comes at the cost of commitments to democratic values and brings U.S. tech closer to China's much-criticized model.

By contrast, a transnationalist position must call out the domestic implications of these security-centric agenda, that government efforts to restrict the use of TikTok would seriously harm free expression and free competition. Such a stance should instead advocate for categorical legislation on all social media platforms—

U.S. or foreign—to combat misinformation, protect online privacy, and enforce parental controls.

Part III: Building a Viable Alternative

As the social credit and TikTok case studies demonstrate, techno-nationalism has shaped U.S. foreign policy thinking around China and had a significant influence on the shape of the policies that have emerged around technology.

This influence has been harmful in a number of respects. First, it has created a pronounced tendency to identify widely shared problems as problems unique to a "Chinese" method of building and deploying technologies. This has led to policies that target foreign companies and individuals while leaving domestic ones free from scrutiny and regulation, even though both may engage in harmful practices.

Second, techno-nationalism has led to the proposal of policies that fail to balance national security concerns with important domestic interests. This includes the preservation of competitive markets for emerging technology, rights of free expression, and the defense of civil rights to privacy and due process. Sometimes, as in the case of Clearview and Palantir, this has been due to a willingness to allow U.S. companies to operate in a more unfettered way though they engage in the same or similar practices to Chinese firms. In other cases, such as the proposed RESTRICT Act, it is because techno-nationalism has shifted norms about the permissible level of government regulation and restriction of speech platforms online.

Third, techno-nationalism has also led to policies that work to erode U.S. competitiveness over time. By narrowly focusing on zero-sum competition over technology as upstream of global competitiveness, techno-nationalism distracts U.S. policymakers from the wide spectrum of areas that the United States will need to compete in to retain its global preeminence in coming decades. This includes the winning of world-class talent globally, ensuring the dynamism and openness of the economy to new upstarts, and the revitalization of U.S. institutions and state capacity. It is these factors that are upstream of technological advantage, rather than the other way around.

What is urgently needed is the construction of a comprehensive and cohesive alternative to the vision of U.S. foreign policy than the one forwarded by the techno-nationalist position. There are three key components to this: emphasizing convergence, reviving techno-optimism, and transnational organizing.

Emphasizing Convergence, Not Divergence

Techno-nationalism sees technology through the lens of geopolitical competition, and as a result has a tendency to draw arbitrary lines between U.S.

and Chinese firms and industries. However, the fact of the matter is that the last few decades have been a period of intense exchange between the United States and China in ideas, financial capital, and technologies. As a result, it is often the case that the structure, outlook, and practices of the technology industry in both countries are frequently more similar than they are different. This is perhaps particularly stark in cases like ByteDance, where many of the company's founding principles and product design ideas came **directly from the rise of social media** in the United States.

Techno-nationalist policies often ignore this history to the detriment of wise U.S. policymaking in two respects. First, they lead to policies that attempt to deal with the societal issues of the technology industry on crude national lines that fail to recognize the shared pathologies that characterize the industry globally. Second, by arbitrarily differentiating policies on national lines, they mask areas where U.S. policymaking may be substantively converging with Chinese policies around technology in ways that are in conflict with democratic values.

There is a need on the part of civil society groups and researchers to highlight these parallels between the United States and China and counter a purely national lens for thinking about technology and technology policy. Doing so would work to better ground the assumptions underlying foreign policy strategy and provoke a broader discussion around the root causes of various social challenges raised by new technologies.

Revitalizing Techno-Optimism

As discussed above, techno-nationalism can be seen as a shift from earlier visions of the role of technology in U.S. foreign policy that emphasized the democratic and commercial potential of the internet and other emerging innovations. While equally focused as techno-nationalism on the pivotal importance of shaping technology as an element of U.S. global power, it implicitly emphasized the competitiveness of markets and the need to preserve values outside a narrow focus on national security.

There was much that was naïve about this earlier techno-optimism discourse. The internet, despite many claims at the time, did not inherently challenge autocracies and empower democratic forces globally. The wide, global competitiveness of many technological markets also became quickly concentrated among a few monopolistic or oligopolistic firms. However, we feel that the deeper values embedded in techno-optimism still remain relevant and viable today, particularly in a project to articulate a cohesive alternative to techno-nationalism.

As part of this, there is an important intellectual project to evaluate and revitalize techno-optimism. For us, this involves a focused effort by activists and intellectuals to revisit the core texts of early 2000s techno-optimism, honestly

critique its failures, and engage in an effort to adapt some of its ideals to the foreign policy problems of the 2020s and beyond.

Transnational Organizing

Techno-nationalism tends to emphasize the harms wrought by technology on vulnerable constituencies abroad rather than domestically. The use of technology in committing the human rights abuses in Xinjiang, for instance, often fails to make links to the highly parallel use of technology on vulnerable communities in the United States. We do not argue that these harms are equivalent; rather, we recognize that China's authoritarian technological capabilities are not unique to China but transcend differences in political systems.

Civil society organizations should work to build transnational bridges to mitigate this gap and challenge these narratives, helping to share knowledge and experiences surrounding the degree to which similar situated groups are experiencing common harms from the deployment of technologies.

This is broader than simply groups in the United States and China. The intersection between rising U.S.-Chinese tensions and technology has had ripple effects globally, impacting populations around the globe as trade and other policy areas have become flashpoints. By fostering a global network of civil society groups, it will be possible to forge a coalition capable of helping to ground an understanding of the harms happening in both the United States and China and to drive advocacy that reflects shared interests beyond the borders of a single nation.

Conclusion

Frameworks matter. Techno-nationalism is a significant force because it has provided a sharp articulation of the exact nature of the competition between the United States and China and the priorities needed for the United States to compete effectively. It has already made a mark on U.S. foreign policy thinking and public discourse and seems likely to exert a growing influence on actual policy in the coming years.

However, the techno-nationalist approach has the potential to produce a great deal of harm relevant to many different constituencies. For human rights groups, techno-nationalism presents a prioritization of national security concerns over a range of interests in civil liberties, privacy, and minority protections. For technologists and entrepreneurs, techno-nationalism seems poised to give a small handful of leading companies a red carpet to policymaker influence and government favoritism. Even for China hawks, techno-nationalism is poised to refocus priorities away from a wide range of different levers outside technology in ensuring U.S. advantage in a future great power conflict.

All these groups have an interest in developing alternatives to the establishment of a U.S. foreign policy consensus in favor of techno-nationalism. By adopting a program emphasizing the connections and parallels between the U.S. and Chinese systems, revitalizing early 2000s techno-optimist thinking, and engaging in genuine organizing across national boundaries, we can build stronger alternatives to guide U.S. foreign policy into the twenty-first century.

NEW AMERICA