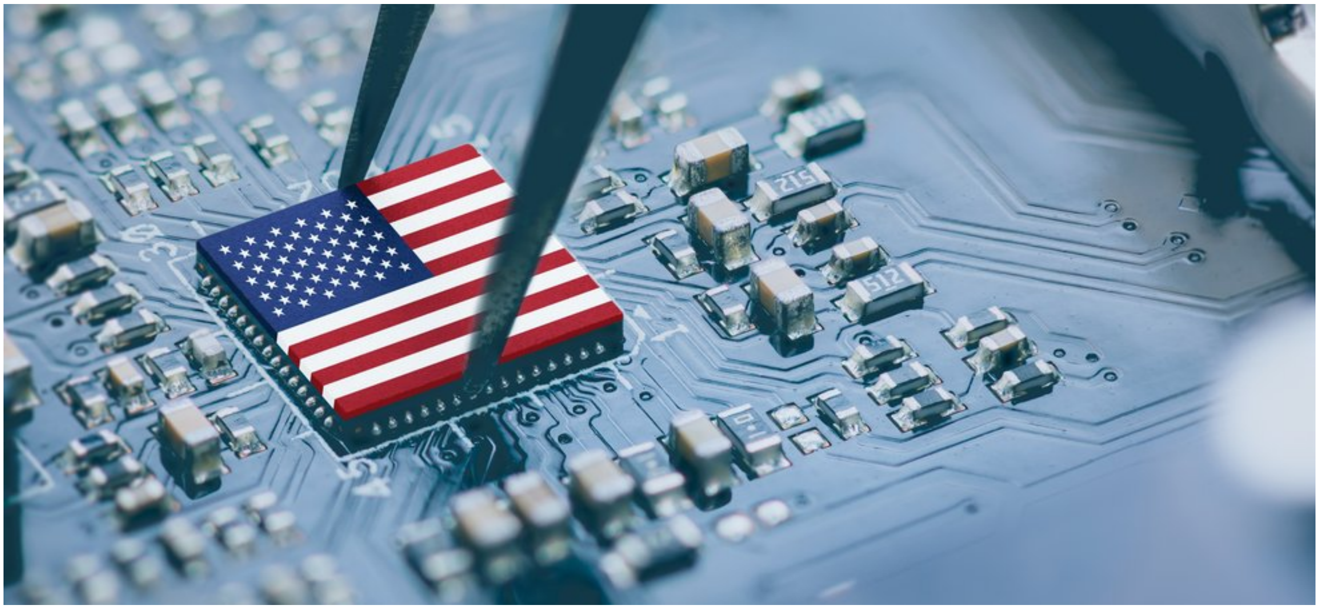

September 2024

Digital Solidarity in U.S. Foreign Policy

Tianyu Fang & Tim Hwang

Open Technology Institute

Last edited on September 04, 2024 at 10:26 a.m. EDT

About the Authors

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

Digital Solidarity in U.S. Foreign Policy: Analyzing Technology Strategy from Clinton to Blinken

Introduction

As Vice President Kamala Harris has begun to outline her vision for American foreign policy, one of the most immediate themes has been the critical role that competition in emerging technologies will play. "I will make sure that we lead the world into the future on space and artificial intelligence," she declared in her speech accepting the Democratic nomination for the presidency, promising that "America—not China—wins the competition for the 21st century" and urging the United States to "strengthen—not abdicate—our global leadership."[1]

Should Harris be elected president in November, it is likely that the doctrine of digital solidarity—which emphasizes technological collaborations with U.S. partners against the notion of digital sovereignty—will guide her administration's diplomatic efforts. In May 2024, Secretary of State Antony Blinken **announced** a series of strategies that repositioned the role of digital technology in U.S. foreign policy. "Today's revolutions in technology are at the heart of our competition with geopolitical rivals. They pose a real test to our security," said Secretary Blinken at the RSA Conference in San Francisco. Additionally, in response to China's geopolitical and technological challenge, the ***International Cyberspace and Digital Policy Strategy*** aims to follow the *2023 National Cybersecurity Strategy* to safeguard an "innovative, secure, and rights-respecting digital future."[2]

Secretary Blinken's strategy, which emphasizes digital solidarity with U.S. partners and allies against Beijing's technological ambitions, has followed the Biden administration's past attempts to curb China's development in critical tech sectors, including **export controls** and an **investment ban** on Chinese companies producing sensitive technologies.

More than a decade ago, the State Department under Secretary Hillary Clinton proposed a set of digital strategies known as "21st-century statecraft." Highlighting the emerging role of internet technology in foreign policy, Clinton first promoted safeguarding internet freedom as a core component of U.S. diplomatic efforts.[3]

In this report, we revisit the State Department's cyberspace strategy under Secretary Clinton. We then focus on the "freedom to connect," which is a framework once championed by civil society, tech corporations, and the foreign policy apparatus of the Obama administration. Assessing the framework's successes, failures, and lessons, we then examine the paradigm shift in U.S. foreign policy's technology strategy under the Biden administration. Lastly, in response to Secretary Blinken's "digital solidarity," we call for a more limited scope of technological competition, a sharpened focus on values rather than actors, and an openness to engage China on standards for emerging technology.

Part I: Internet Freedom Revisited

Toward the end of the Cold War, Francis Fukuyama contended that major ideological contests had come to a conclusion. The Soviet Union would soon collapse, the European Union was becoming a reality, and China signaled its embrace of market capitalism. The neoconservative impulse that U.S. foreign policy should promote liberal capitalism and democracy abroad through interventionism was on the rise. Meanwhile, modernization theorists argued that as authoritarian countries embraced the free market and achieved economic prosperity, political liberalization would inevitably follow. Without a viable ideological rival, the globalization of liberal democratic systems seemed more possible.

The triumphalism of the liberal universalists in the 1990s, however, was met with widespread skepticism following the turn of the century. Under President George W. Bush, the U.S. invasion of Iraq in the name of democratic promotion resulted in domestic criticism and international outcry. In Russia, Vladimir Putin's consolidation of power diminished hopes for its further democratization. Despite China's fast growth, the prospects of political liberalization appeared distant. Having witnessed the stagnation and reversals in global democratization in the 2000s, political scientists were increasingly concerned about buzzwords like "democratic recession" and "authoritarian resilience."[4] The 2008 financial crisis only further fueled global skepticism of the Washington Consensus, and commentators wondered if the "China model" would come to the rescue.

At this moment of disillusionment, the booming sector of consumer internet offered both a new model for the post-2008 economy and a source of renewed hope in global liberalism. "The free flow of information and ideas over digital technologies is in our national and global interests," concluded the Department of State in 2010.[5] "It is important for economic growth; for U.S. diplomatic relationships; for building sustainable democratic societies; and for meeting global challenges in the years and decades ahead."[6] During the Cold War, Washington had set up radio stations—the **Voice of America** and **Radio Free Europe**, for example—to spread liberal democratic values in communist countries. On the web, this effort was to be decentralized. Citizens around the world could break through censorship restrictions, build communities, and organize digitally. While liberal ideas traveled to authoritarian states, social networks empowered their realization. If the free market couldn't loosen the grips of the autocrats, a vibrant, digitally networked civil society just might.

The Fifth Freedom

The internet did help coordinate anti-authoritarian movements. After Moldova's 2009 parliamentary election, young Moldovans rallied fellow citizens to oppose the governing Communist Party using Twitter hashtags. In the 2009 Green Movement, Iranian activists coordinated online to protest what they believed to be a fraudulent election. Mass protests broke out in Tunisia in 2011 following the self-immolation of a street vendor, and soon, activists across the Arab world led demonstrations and uprisings. Collectively known as the Arab Spring, these movements were facilitated by internet platforms where citizens connected with one another, shared organizing tactics, and broadcasted updates in real time. Noticing the role of the web, the press was quick to dub these movements "Twitter revolutions,"[7] despite the criticism and skepticism of these techno-solutionist narratives at the time.[8]

U.S. diplomacy swiftly captured the global adoption of the internet for democratization. Drawing upon President Franklin D. Roosevelt's "**Four Freedoms**" speech, then Secretary of State Hillary Clinton argued in January 2010 that with the advancement in global communication technologies, a fifth freedom must be secured—the freedom to connect.[9] It was the U.S. government's obligation to ensure that "governments should not prevent people from connecting to the internet, to websites, or to each other." To Clinton, an open internet would undermine dictatorships, transform societies, and provide global networks that could facilitate disaster relief, medical access, and economic development.[10] The idea that U.S. foreign policy should secure the global "freedom to connect" was based on several key assumptions.

First, it narrowly focused on the internet as the core technological vehicle. Technology in the 2000s wasn't just comprised of information tech, yet the internet dominated the foreign policy imagination. Secretary Clinton **argued** that if the Berlin Wall symbolized a divided world of the postwar era, "the new iconic infrastructure of our age is the internet. Instead of division, it stands for connection."[11] This connection, however, relied on an assemblage of technological infrastructure that was vulnerable to political meddling, supply chain disruptions, and corporate surveillance—from government-controlled cables and mass-produced handheld devices to corporation-run servers and platforms.

Second, it held that the internet was inherently liberatory and democratizing. U.S. observers long surmised that government censorship of the web would simply be unsustainable. As early as 2000, President Bill Clinton said there was "no question China has been trying to crack down on the Internet," yet doing so would be "trying to nail jello to the wall."[12] Internet researcher Ethan Zuckerman argued in 2008 that calls for political activism and cat memes are shared on the same platforms; for governments to censor the former, they risk radicalizing citizens going online for the latter.[13] As new, iterative technological tools render it increasingly difficult for governments to censor information on the web, U.S. foreign policy believed that a full-fledged censorship apparatus would simply be too costly in a cat-and-mouse game.

Third, it assumed that the United States and other liberal democracies would dominate digital technologies. U.S. government officials and Silicon Valley entrepreneurs alike conjectured that internet censorship and the absence of political transparency would slow down technological and economic development in tightly controlled information regimes. Recognizing China's growing number of internet users, Secretary Clinton **noted** in 2010 that "countries that restrict free access to information or violate the basic rights of internet users risk walling themselves off from the progress of the next century." [14] Without transparent information and news reports, "investors will have less confidence in their decisions over the long term."[15] Eric Schmidt, then CEO of Google, told a reporter that it was not possible to "build a modern knowledge society" with the kind of censorship apparatus that the Chinese government had deployed.[16] The presumption that China could not innovate implied that global internet services would always be in democratic hands; even when Chinese platforms outcompeted U.S. rivals, their success would be confined to China's own walled garden.

Lastly, it assumed that corporate, government, and civil society interests would align on the issue of global democratic promotion. Clinton highlighted **Google's exit from China** as an example of U.S. technology companies "making the issue of internet and information freedom a greater consideration in their business decisions."[17] Whereas the tech companies in Silicon Valley hadn't always seen eye to eye with the U.S. government, they conveniently agreed on the democratizing potential of internet technology. Mark Zuckerberg, chairman and CEO of the social media company Meta, **told** a reporter in 2009 that the vision of "a world that was more open" had inspired him to start Facebook. Openness, he said, "fundamentally affects a lot of the core institutions in society—the media, the economy, how people relate to the government, and just their leadership."[18] In the eyes of the U.S. government, which had long feared the disruptive power of California's technologists, the same companies that were at the time entangled in legal battles at home could be enlisted in Washington's global scramble for democratic universalism. By marrying the normative claims and foreign policy priorities of the U.S. government with the commercial interests of rapidly expanding tech corporations, the "freedom to connect" mapped global freedom of speech onto the trade issue of market access for Silicon Valley.

The End of the Open Web?

The outcomes of Clinton's "internet freedom" campaign defied its techno-optimistic advocates. Despite its initial popularity, "internet freedom" as a diplomatic rhetoric faded for several reasons.

First, it was largely a self-defeating prophecy since authoritarian governments were able to adapt faster and better than the U.S. foreign policy community anticipated. Authoritarian governments, long wary of U.S.-backed regime changes, thought of the open internet as a vulnerability to their regime stability—just as U.S. officials and journalists had advertised it to be. Countries like China and Iran quickly bolstered their censorship infrastructure to curtail access to foreign websites and platforms. As Beijing successfully nailed jelly on the wall, it adopted an alternative version of the internet: Under Xi Jinping's "internet sovereignty," nation-states should control and regulate cyberspace within their own borders.[19] In addition to censorship, authoritarian actors have also leveraged the internet to crack down on dissent and consolidate power.

Second, wide skepticism of tech companies at home fueled pessimism, making the hope of reshaping the international order through the internet a less credible perspective. Compared to their advertised zeal for democratic ideals, the growing tech giants of Silicon Valley were more committed to profits. As early as 2012, internet freedom expert Rebecca MacKinnon argued that the private corporations masquerading as public spheres simply lacked mechanisms of public accountability.[20] As media historian Fred Turner has aptly **observed**, the platforms' "ability to simultaneously solicit and surveil communication has not only turned the dream of individualized, expressive democracy into a fountain of wealth. It has turned it into the foundation of a new kind of authoritarianism."[21] In the United States, corporate practices around data privacy, parental control, and algorithmic transparency on these seemingly public forums have raised political concerns. The social media platforms that once helped put Barack Obama into the White House and allowed Tunisian protesters to rally against their government were later associated with aiding Russian interference, promoting extremism, and facilitating a genocide in Myanmar.

Finally, there was a broad recognition that the openness of the internet was not, as it was previously believed, unconditionally liberating. As many critics have rightly pointed out, the buzzword "internet freedom" was often culpable of technological determinism; it centered on the technological tools rather than the regional context, political strategies, complex relations of power, and pathways toward new orders after revolutions. In 2011, Evgeny Morozov, a researcher and writer who focuses on technology and politics, argued against "cyber-utopianism" and "internet-centrism," both of which mistakenly frame technology as deterministically "good." Instead, he called for a strategy of "cyber-realism" that recognizes that the internet is "poised to produce different policy outcomes in different environments" and prioritizes making the internet "an ally in achieving specific policy objectives."[22]

As Beijing touted its vision of "internet sovereignty" and thrived economically and geopolitically, support for internet freedom also faded in liberal democracies. For one, illiberalism has not necessarily curbed Beijing's ability to innovate and dominate global markets. While most major platforms were, at one point, run by Silicon Valley, today legislators in Washington fear that China can leverage apps like the Bytedance-owned TikTok to gather intelligence and covertly influence American minds. As the **impending ban on the platform** shows, the United States was willing to abandon its original rhetoric of "freedom to connect" to serve national security and economic protectionism. Meanwhile, U.S. allies have demonstrated similar tendencies to embrace a sovereignty-centric approach, especially as the European Union's "digital sovereignty" framework prioritizes EU autonomy over internet data and technology regulations in cyberspace.[23]

Part II: The Pivot to Digital Solidarity

In retrospect, Secretary Clinton's hopes for global democratization by the internet seem naive at best. Amid the disillusionment with the internet's democratizing promises, the unilateralism of the Trump administration, and Beijing's challenge to U.S. technological hegemony, U.S. foreign policy under President Joe Biden has adopted a different set of tools to regain leadership in the geopolitical scramble for global tech supremacy. These parameters were consolidated in Secretary Antony Blinken's appeal to "digital solidarity." The strategy "recognizes that all who use digital technologies in a rights-respecting manner are more secure, resilient, self-determining, and prosperous when we work together to shape the international environment and innovate at the technological edge."[24]

Digital solidarity, however, was not the State Department's invention. Proposed by tech policy expert Pablo Chavez in a 2022 *Lawfare* essay, it was **coined** as a counter to digital sovereignty, a vision shared not just by China and Russia but also the European Union, whose quest for technological self-determination increasingly favored a closed digital ecosystem. Digital solidarity, by contrast, is an "alternative path to achieving technological self-determination through partnerships and alliances among open, democratic, and rule-bound societies."[25]

We identify two important pillars of the current administration's tech strategy for geopolitics that differ significantly from the Obama era.

First, digital solidarity relies on U.S. partners and allies to create an alternative set of technological infrastructure, standards, and norms to

that of U.S. competitors and adversaries. While the "freedom to connect" assumed that U.S. internet platforms would succeed in a global free market and that American-style liberalism would dominate in the marketplace of ideas, the Trump and Biden administrations have grappled with the U.S. economy's reliance on Chinese-controlled nodes of supply chains. The result has been an approach that abandons a global vision for technology and instead attempts to cordon off a coterie of allied nations from the threats posed by geopolitical competitors. Just as President Biden attempts to renew U.S. commitment to liberal-democratic allies through initiatives such as the Summit for Democracy,[26] the framework of digital solidarity prioritizes the global risks of emerging technologies and the establishment of standards and norms along with partners and allies. These norms are seen as not universal but in contest with U.S. adversaries and competitors. Importantly, unlike the utopian aspirations for a globally connected digital ecosystem under Clinton, digital solidarity accepts a balkanized technological landscape where non-autocracies are able to maintain an alternative technological stack.

Second, while the Clinton era focused on the internet as the core battleground for U.S. diplomatic power, the Blinken strategy declares American interests in a far wider range of strategic technologies. The material and sociological infrastructure that undergirded the "social media revolutions" was, importantly, prone to control by authoritarian governments. To the Blinken administration, cyberspace security is predicated upon lower layers of the technology "stack," and thus the underlying hardware—from subsea cables and 5G networks to cloud computing—must be recognized as critical battlegrounds for U.S. initiatives.[27] This development should be viewed in the light of security concerns revealed in the ongoing U.S.-China technological competition. Worries about data security and espionage have raised concerns about Huawei's potential involvement in 5G infrastructure in Europe, Chinese subsea cable routes, and Beijing's semiconductor ambitions.

Lessons from the Past

The connections between digital solidarity and internet freedom could not be more evident. "Blinken's speech is replete with references to openness, globalization, and a more democratic world," observed Akash Kapur, a senior fellow at New America's Planetary Politics initiative. "These passages are infused with an idealism and optimism that hark back to a certain lost innocence, a golden era before the network's promise was sullied by the depredations of Big Tech and state authoritarianism."[28]

But if Secretary Blinken's approach wanted to rectify the errors of the Clinton era's utopianism, we argue that the vision for "digital solidarity" as it is currently articulated relies upon a series of risky and unsubstantiated assumptions—not unlike the internet optimism of the Clinton era. In this light, the successes and failures of the "freedom to connect" offer valuable lessons for policymakers of the current administration as well as the next.

First, the digital solidarity strategy incorrectly presumes a dichotomy between two camps: Democracies produce "rights-respecting" technology,[29] while authoritarian countries produce technology that intends to harm. Technological abuse and human rights violations occur in transnational contexts and transcend the simplified binary of regime types. Take facial recognition as an example. The People's Republic of China (PRC) has a track record of using facial recognition technologies to surveil, discriminate, incarcerate, and persecute ethnic minorities and political dissidents. Yet, as many scholars have noted, the Chinese government has learned many of its tactics from the expanded security apparatus in the United States-led war on terror.[30] Today, U.S. companies such as **Palantir Technologies** and **ClearviewAI** offer surveillance software to American police officers. Israeli authorities have **used facial recognition** the movement of Palestinians, and human rights organizations have **voiced concerns** over the Indian government's digital surveillance apparatus.

To attentive ears, the narrative of "rights-respecting technology" evokes the hypocrisy of the push for the "freedom to connect." As Clinton rightly condemned internet censorship in Iran and bashed China's cyberattacks in the early 2010s, the U.S. National Security Agency was engaged in global mass surveillance through the internet,[31] just as the Indian government made attempts to censor "objectionable content" on the web.[32] "American corporations are major suppliers of software and hardware used by all sorts of governments to carry out censorship and surveillance—and not just dictatorships," noted Rebecca MacKinnon in 2012.[33] Without meaningful efforts to address and regulate rights-disrespecting technologies, which are currently adopted by the United States government and its partners, the security-centric approach risks further accusations of hypocrisy and could undermine universal democratic values. Regulations that center national origins obscure the transnational nature of technological misuse and jeopardize civil liberties in the United States; whereas tech legislations often rightly target Chinese companies for their rights violations, U.S. companies behaving similarly are likely seen as boosting American competitiveness.

Second, it would be a mistake to assume that Beijing holds inherently different values when it comes to norm- and standard-setting in emerging technology vis-à-vis the U.S. and its partners and allies. On the contrary, current Chinese regulations on artificial intelligence, digital privacy, and clean energy often resemble existing and proposed Western frameworks and are, in many cases, more progressive than U.S., British, and European counterparts.[34] In these areas, a global consensus on standardized norms is critical to preventing technological risks, building safety guardrails, and scientific collaboration. Where security is not the top priority, the focus on norm-setting with only U.S. partners and allies potentially neglects common interests with China and creates distrust and chasms on issues pertaining to a collective future.

The rise in China's tech sector and discussions about Beijing's manufacturing overcapacity also mean that the United States should seek to benefit from areas where Chinese companies are ahead. The recent progress in Chinese electric vehicle (EV) manufacturing, for instance, has presented an opportunity to address climate issues that also confront the United States and its partners. Despite the potential trade disputes, electric cars made with Chinese batteries are unlikely to be a threat to U.S. national security, nor are they antithetical to liberal-democratic values. In Germany, the automaker Volkswagen **has invested in Xpeng**, a leading Chinese EV firm, to accelerate EV production in Europe; its European peers **have followed** suit. In the United States, however, Ford's attempt to create a joint-venture factory with Chinese EV battery producer CATL was **criticized** by Republican politicians. As the Biden administration **limits the access of U.S. capital to Chinese technology**, American competitiveness is hindered by the inability to borrow from advancements in the PRC.

Recommendations

Both Clinton's "freedom to connect" and Blinken's "digital solidarity" are problematic approaches for fostering and maintaining an "open, inclusive, secure, and resilient digital ecosystem." If the United States is serious about such an objective, there should be a new doctrine that is informed by lessons from the previous two decades. Such a doctrine would incorporate three major components.

First, Washington should practice caution in expanding the scope of foreign policy involvement in technology. Whereas the Clinton perspective mistakenly centered the internet as the central technology of American foreign policy, Blinken's "stacks" approach risks over-intervention across too broad a range of technologies. While Blinken has stated that he prefers a "small yard, high fence" approach to sensitive technologies,[35] the yard has increased in size in recent years.

Aside from a handful of critical sectors, attempts to fully decouple from Chinese industries are neither preferable nor practically viable. On the one hand, the United States must recognize the necessity to engage with the PRC in non-military technological applications where common interests are found. Geopolitical contests should not be the sole driver of technology policy, which must also prioritize economic vitality, democratic accountability, and climate preparedness. Scientific, commercial, and academic collaborations—especially those in areas such as climate tech and public health—should be viewed as assets that strengthen U.S. technological openness and resilience. Partners and allies that the U.S. seeks solidarity with recognize this reality and have been more open to collaborating with their Chinese counterparts.

Second, the United States should remain committed to supporting open, resilient technological values, regardless of actors. The Clinton administration was right to identify the "freedom to connect" as a global, not regional, set of principles; these attempts would have been far more successful had they been practiced with consistency across borders. In creating digital solidarity with democratic values, not just nation-states, the United States should be willing to assess and regulate harmful practices by American corporations, government agencies, and institutions as well as those by its partners and allies. This means placing producers of rights-disrespecting technology in the United States under the same scrutiny as it would Chinese counterparts.

And lastly, the United States should push to depoliticize standard-setting and norm-setting processes. Foreign policy must recognize that, in the face of emerging technology, a global consensus on technological norms and guardrails is often more important than national priorities. Technological risks cannot be averted by creating a balkanized ecosystem. Rather than viewing technological standards as arenas to push for national interests, Washington and Beijing alike should take a technocratic, neutral approach that establishes global common ground. China's **participation** at the U.K. AI Safety Summit, for example, signaled potential for consensus and engagement.

Conclusion

Like Secretary Blinken, we believe the utopianism of the Clinton era—that technology should be open and resilient—is worth preserving as the guiding light of U.S. foreign policy. These values, however, cannot be defended by attempting to engineer an alternative technological universe through a narrow vision that prioritizes "solidarity" with allies above all. This will skew the United States toward overlooking violative uses of technology at home and among allies while blocking opportunities for genuine collaboration with geopolitical rivals. For the United States to retain its global tech leadership, Washington must hone its ability to collaborate and integrate with not just its friends but also adversaries and competitors on critical issues confronting international technological development.

Notes

[1] Kamala Harris, “Remarks by Vice President Harris During Keynote Address at the Democratic Nation Convention,” (keynote address, 2024 Democratic National Convention, Chicago, IL, August 22, 2024), https://www.whitehouse.gov/briefing-room/speeches-remarks/2024/08/22/remarks-by-vice-president-harris-during-keynote-address-at-the-democratic-nation-convention/.

[2] Andrew J. Blinken, “Technology and the Transformation of U.S. Foreign Policy,” (speech, RSA Conference, San Francisco, CA, May 6, 2024), https://www.state.gov/technology-and-the-transformation-of-u-s-foreign-policy/.

[3] Hillary Rodham Clinton, “Remarks on Internet Freedom,” (remarks at the Newseum, Washington, DC, January 21, 2010), https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[4] See, for example, Larry Diamond, *The Spirit of Democracy: The Struggle to Build Free Societies throughout the World* (New York: Times Books, 2008); Andrew J. Nathan, “China's Changing of the Guard: Authoritarian Resilience,” *Journal of Democracy* 14, no. 1 (January 2003): 6–17, https://doi.org/10.1353/jod.2003.0019.

[5] Bureau of Public Affairs, “Internet Freedom in the 21st Century: Integrating New Technologies into Diplomacy and Development,” U.S. Department of State, February 4, 2010, https://2009-2017.state.gov/r/pa/scp/fs/2010/136702.htm.

[6] “Internet Freedom in the 21st Century: Integrating New Technologies into Diplomacy and Development,” https://2009-2017.state.gov/r/pa/scp/fs/2010/136702.htm.

[7] Alina Mungiu-Pippidi and Igor Munteanu, “Moldova's ‘Twitter Revolution,’” *Journal of Democracy* 20, no. 3 (2009): 136–42, https://www.journalofdemocracy.org/articles/moldovas-twitter-revolution/; Luke Harding, “Moldova Forces Regain Control of Parliament after ‘Twitter Revolution,’” *The Guardian*, April 8, 2009, https://www.theguardian.com/world/2009/apr/08/moldova-protest-election-chisinau; Jared Keller, “Evaluating Iran's Twitter Revolution,” *The Atlantic*, June 18, 2010, https://www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/.

[8] See, for example, Adam Segal, “The Chinese Internet Century,” *Foreign Policy*, April 11, 2010, https://web.archive.org/web/20100411023359/https://foreignpolicy.com/articles/2010/01/26/the_chinese_internet_century.

[9] Clinton, “Remarks on Internet Freedom,” https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[10] Clinton, “Remarks on Internet Freedom,” https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[11] Clinton, “Remarks on Internet Freedom,” https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[12] “Clinton's Words on China: Trade Is the Smart Thing,” *New York Times*, March 9, 2000, https://www.nytimes.com/2000/03/09/world/clinton-s-words-on-china-trade-is-the-smart-thing.html.

[13] Ethan Zuckerman, “The Cute Cat Theory Talk at ETech,” *Ethan Zuckerman* (blog), March 8, 2008, https://ethanzuckerman.com/2008/03/08/the-cute-cat-theory-talk-at-etech/.

[14] Clinton, “Remarks on Internet Freedom,” https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[15] Clinton, “Remarks on Internet Freedom,” https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[16] Josh Rogin, “Eric Schmidt: The Great Firewall of China Will Fall,” *Foreign Policy*, July 9, 2012, https://

foreignpolicy.com/2012/07/09/eric-schmidt-the-great-firewall-of-china-will-fall/.

[17] Clinton, "Remarks on Internet Freedom," https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

[18] Fred Volgelstein, "The Wired Interview: Facebook's Mark Zuckerberg," *Wired*, June 29, 2009, https://www.wired.com/2009/06/mark-zuckerberg-speaks/.

[19] Johanna Costigan, *Determining the Future of the Internet: The U.S.-China Divergence* (New York: Asia Society, January 19, 2023), https://asiasociety.org/policy-institute/determining-future-internet-us-china-divergence.

[20] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (New York: Basic Books, 2013).

[21] Fred Turner, "Machine Politics: Does the Rise of Index Funds Spell Catastrophe?," *Harper's Magazine*, January 2019, https://harpers.org/archive/2019/01/machine-politics-facebook-political-polarization/.

[22] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, 1st ed (New York: Public Affairs, 2011), 319–20.

[23] Tambiama Madiega, *Digital Sovereignty for Europe* (European Parliament, July 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

[24] *United States International Cyberspace & Digital Policy Strategy* (U.S. Department of State, May 6, 2024), https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

[25] Pablo Chavez, "Toward Digital Solidarity," *Lawfare*, June 28, 2022, https://www.lawfaremedia.org/article/toward-digital-solidarity.

[26] "FACT SHEET: Delivering on the Biden-Harris Administration's Commitment to Democratic Renewal at the Third Summit for Democracy," The White House, March 20, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/20/fact-sheet-delivering-on-the-biden-harris-administrations-commitment-to-democratic-renewal-at-the-third-summit-for-democracy/. See also Secretary Blinken's vision for a "league of democracies": Antony J. Blinken and Robert Kagan, "'America First' Is Only Making the World Worse. Here's a Better Approach," Brookings, January 4, 2019, https://www.brookings.edu/articles/america-first-is-only-making-the-world-worse-heres-a-better-approach/.

[27] The approach "uses the appropriate tools of diplomacy and international statecraft across the entire digital ecosystem. This ecosystem includes but is not limited to hardware, software, protocols, technical standards, providers, operators, users, and supply chains spanning telecommunication networks, undersea cables, cloud computing, data centers, satellite network infrastructure, operational technologies, applications, web platforms, and consumer technologies as well as Internet of Things (IoT), artificial intelligence (AI) and other critical and emerging technologies." See *United States International Cyberspace & Digital Policy Strategy*, https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

[28] Akash Kapur, "What Is Digital Solidarity, and Why Does the U.S. Want It?," *Foreign Policy*, July 31, 2024, https://foreignpolicy.com/2024/07/31/digital-solidarity-rsa-conference-blinken-speech/.

[29] Blinken, "Technology and the Transformation of U.S. Foreign Policy," https://www.state.gov/technology-and-the-transformation-of-u-s-foreign-policy/.

[30] According to Darren Byler and Carolina Sanchez Boe, "While the Chinese system is unique in terms of its scale and the depth of its cruelty, terror capitalism is an American invention, and it has taken root

around the world." See Darren Byler and Carolina Sanchez Boe, "Tech-Enabled 'Terror Capitalism' Is Spreading Worldwide. The Surveillance Regimes Must Be Stopped," *The Guardian*, July 24, 2020, https://www.theguardian.com/world/2020/jul/24/surveillance-tech-facial-recognition-terror-capitalism; Darren Byler, *Terror Capitalism: Uyghur Dispossession and Masculinity in a Chinese City* (Durham, NC: Duke University Press, 2022); Sean R. Roberts, *The War on the Uyghurs: China's Internal Campaign against a Muslim Minority* (Princeton, NJ: Princeton University Press, 2020).

[31] "Germany, Brazil to Propose Anti-Spying Resolution at U.N.," Reuters, October 26, 2013, https://www.reuters.com/article/world/germany-brazil-to-propose-anti-spying-resolution-at-un-idUSBRE99P01D/.

[32] "Facebook and Google Remove 'offensive' India Content," *BBC News*, February 6, 2012, https://www.bbc.com/news/world-asia-india-16903765.

[33] Rebecca MacKinnon, "Internet Freedom Starts at Home," *Foreign Policy*, April 3, 2012, https://foreignpolicy.com/2012/04/03/internet-freedom-starts-at-home/.

[34] For example, see Matt Sheehan, *China's AI Regulations and How They Get Made* (Washington, DC: Carnegie Endowment for International Peace, July 10, 2023), https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made; Matt Sheehan, "What the U.S. Can Learn From China About Regulating AI," *Foreign Policy*, September 12, 2023, https://foreignpolicy.com/2023/09/12/ai-artificial-intelligence-regulation-law-china-us-schumer-congress/.

[35] Blinken, "Technology and the Transformation of U.S. Foreign Policy," https://www.state.gov/technology-and-the-transformation-of-u-s-foreign-policy/.