CSPC

CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

SECURING DIGITAL FREEDOM

MARCH 2023

CSPC CENTER FOR THE STUDY OF THE PRESIDENCY & CONGRESS

SECURING DIGITAL FREEDOM

MARCH 2023

The Hon. Glenn Nye
President & CEO

The Hon. Mike Rogers
David M. Abshire Chairholder

Dan Mahaffee
Senior Vice President, Director of Policy

Joshua Huminski
Director, CSPC Mike Rogers Center for Intelligence & Global Affairs

Erica Ngoenha
Vice President for Programs & External Affairs

Hidetoshi Azuma
Ethan Brown
Samantha Clark
Rob Gerber
Andy Keiser
James Kitfield
Joshua Walker
Zaid Zaid
CSPC Senior Advisors & Fellows

Table of Contents

Introduction

As more and more of our lives are lived in the digital domain, the issue of digital freedom is becoming more and more important to policymakers. Their citizens are increasingly grappling with ever-present social media, reliance on digital services powered by users' data, growing digital surveillance by public and private actors, and a greater reliance on networked digital systems. These trends are present in both free societies and authoritarian regimes. They increasingly compete to determine technical standards, political frameworks, and cultural norms for the use of these technologies.

Free societies are built on cornerstones of trust—trust between citizens, trust in commercial transactions, trust in media, and trust in civic and state institutions. Those same cornerstones apply in the digital domain and digital society, where cultural trends, political discourse, and commercial activity all increasingly take place.

On the global stage, much of the discussion is about the competition for control of and leadership in advanced technologies. Artificial intelligence, facial recognition, and future digital infrastructure are some of the main areas of technological competition. Here the competition is often focused on who will be the first not only to discover a technology but also achieve widespread commercial adoption. Still, it is not simply about being the first to a technology, but how it is applied.

Take for example, an intersection equipped with the latest in networked "smart" technology: video analytics, artificial intelligence, networked infrastructure, etc. In a pilot program underway as a joint venture with Japanese commercial company NEC and Virginia Tech University, such a smart intersection project demonstrated how traffic signals could respond to freeze traffic should a pedestrian or cyclist be incapacitated or immobilized. That same technology and related ones are used in China, with some public safety applications, but also to track dissidents, enforce "social credit" scores, and identify protestors for arrest. In this sense, it is less about the specific technology, but to what end it is used.

However, for many countries beyond the west and China, this global technology competition is not the binary that policymakers in Washington or Beijing might imagine it to be. Many countries, including U.S. partners and allies, have varying approaches to digital freedom. Others hope to choose from a mix of U.S. and Chinese technology—while also developing their own technology, applying their own solutions, and taking ownership of their own digital future. While we may speak of digital freedom as a matter of individual rights, others will counter that digital freedom is not an individual matter, but rather a country's "digital sovereignty" to choose its own technological path, manage its citizens' data, and build its own technological ecosystem. It may also be tempting to but up barriers of our own, or choose digital protectionism over global engagement.

That said, the internet is a global common. That global common is in danger as many authoritarian regimes, or even hybrid ones, successfully separate their nations from the global internet. In their own countries and in international fora, these regimes seek to build the physical infrastructure and legal and regulatory frameworks for a digital society controlled by the government. How the United States and like-minded nations can continue to protect an internet "of, by, and for the people".

Zooming in from the global stage, within many countries the topics falling under the umbrella of digital freedom and digital society are largely the same: countering disinformation, addressing policymakers' and citizens' concerns about big tech, protecting users' data, and ensuring that the underlying digital infrastructure is secure. Here, free societies and authoritarian regimes are competing over their respective models and solutions for these challenges. Ensuring digital freedom will require free societies to put forth superior solutions.

From late 2022 into 2023, the Center for the Study of the Presidency & Congress has examined these topics and how U.S. and allied policymakers can ensure and promote digital freedom. First, it is important to understand just how authoritarian regimes like China, Russia, and others seek to build their models for digital control, and what that means for digital freedom. Then in identifying policy solutions for global and domestic digital freedom, the following is as fundamental to the digital world as it is to the physical one: trust is the coin of the realm. Digital freedom requires trust in the information that we see, trust in the infrastructure upon which it is transmitted, and trust in how platforms and social media present us information, and, often, use our data in exchange.

This report reflects, and respects, the off-the-record nature of private discussions, combined with open-source research, public events, and the analysis of CSPC staff, advisors, and fellows. The report looks at the models of digital repression and control employed by Beijing and Moscow, before looking at how the U.S. and our allies and partners can counter with their own solutions to protect critical infrastructure, reverse trends eroding trust in digital society, and present positive solutions towards global digital freedom. Portions of this report draw from the analysis of CSPC op-eds, white papers, and our Friday News Roundup weekly news analysis. Our analysis of legislation is not meant to be exhaustive—nor endorse legislation—but to track the progress of substantive, and likely, Geotech policymaking and implementation.

China's Digital Regime; Now Honed by COVID Controls

If there is a model for a digital society that is anathema to digital freedom, it is the model promoted by the Chinese Communist Party (CCP). This contest for the future of digital society and digital freedom is part and parcel of a broader technological, economic, and geopolitical competition between the United States and a growing coalition of its western partners—albeit to very differing degrees of the perception of the economic and/or security threat from the policies of the Chinese leadership. Other countries seek to avoid a choice between Beijing's or Washington's strictures.

That said, global perceptions of the CCP have changed due to a range of factors—from the outbreak of the COVID pandemic to repression in Hong Kong and Xinjiang to Xi Jinping's consolidation of power. There has also been increased attention to the CCP's digital model, from the use of social credit scores to online censorship, to the risks posed by installing Chinese-based firms' hardware in critical infrastructure or using Chinese-based apps. While this report will discuss in a later section some countries' responses to concerns about hardware providers like Huawei and ZTE or social media apps like TikTok, the underlying concern comes from the legal strictures the Chinese Communist Party employs to compel cooperation from companies (both Chinese and foreign) on national security matters and the growing interference by the party in private sector matters.

In the CSPC December 2020 Geotech report, the nature of this legal system was noted, as well as how it combines with China's Military-Civil Fusion (MCF) policies in creating the CCP technology model and the underlying realities of the Chinese Communist model for digital society:[1]

> The Counterespionage, Cybersecurity, and Intelligence Laws have put together a network of strictures designed to compel cooperation with Chinese state agencies. Article Seven of the Intelligence Law, states that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law;" Article Fourteen states that "state intelligence work organs, when legally carrying forth intelligence work, may demand that concerned organs, organizations, or citizens provide needed support, assistance, and cooperation."[2]

[1] Mahaffee et al., "Geotech: Ensuring Free Societies' Innovation Leadership." CSPC. December 2020. https://static1.squarespace.com/static/5cb0a1b1d86cc932778ab82b/t/5fda6145b2f3a803a1765706/1608147272794/Geotech_Ensuring+Free+Societies%27+Innovation+Leadership+Report+Dec+2020.pdf

[2] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense." *Lawfare*. July 20, 2017. https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

> These close ties between the CCP and Chinese firms have been further strengthened by measures to promote "Military-Civil Fusion" and increase the role of CCP cadres in the private sector. Along with programs like Made in China 2025—designed to foster leadership in key industries—Military-Civil Fusion, or MCF, aims to integrate advances in key technologies, including artificial intelligence and advanced materials engineering, with their military applications. In the words of the U.S.-China Economic and Security Review Commission:
>
> *The Chinese government's military-civil fusion policy aims to spur innovation and economic growth through an array of policies and other government-supported mechanisms, including venture capital (VC) funds, while leveraging the fruits of civilian innovation for China's defense sector. The breadth and opacity of military-civil fusion increase the chances civilian academic collaboration and business partnerships between the United States and China could aid China's military development*.[3]

Combined with these legal structures and MCF policies, the CCP has also tightened the reins on private industry. The most visible evidence of this has been the crackdown on business leaders, with the disappearance of tycoons in tech, real estate, energy, and banking indicating they have fallen afoul of the regime. This has chilled the overall business environment, as the CCP under Xi Jinping increasingly sees private enterprise as subordinate to the party's aims. September 2020's "Opinion on Strengthening the United Front Work of the Private Economy in the New Era" started a new structure that Chinese leaders have described as "modern private enterprise with Chinese characteristics." By announcing this the CCP has laid the groundwork for a greater role for CCP leadership within the management of private firms.[4] Since then the consolidation of party control of and influence within China's private sector has grown, and, during his March 6, 2023, speech to Chinese private industry in which Xi blamed "U.S. containment, encirclement and suppression" for China's economic woes, Xi again reiterated that private industry exists to serve the party's priorities for national security.

[3] U.S.-China Economic and Security Review Commission, "2019 Report to Congress: Chapter 3 Section 2 – Emerging Technologies and Military-Civil Fusion – Artificial Intelligence, New Materials, and New Energy." Accessed October 20, 2020, & February 17, 2023. https://www.uscc.gov/sites/default/files/2019-11/Chapter%203%20Section%202%20-%20Emerging%20Technologies%20and%20Military-Civil%20Fusion%20-%20Artificial%20Intelligence,%20New%20Materials,%20and%20New%20Energy.pdf

[4] Scott Livingston, "The Chinese Communist Party Targets the Private Sector." Center for Strategic and International Studies, October 8, 2020, accessed February 17, 2023. https://www.csis.org/analysis/chinese-communist-party-targets-private-sector

This model stands in stark contrast to the digital and tech development model in the United States and like-minded countries, where the key priority for the private sector lies in serving their customers and bringing returns to shareholders, rather than the priorities of the state or party. There is, of course, a healthy role for the state of transparent regulation, protecting consumers, and ensuring the rule-of-law and due process when applied to digital society, but this state-led model creates a level of digital control, both over data and the utilization of hardware, that threatens digital freedom.

The Party Monopoly on Data

Since then, as Beijing's policymakers have sought to push ahead with leadership in strategically critical technologies such as semiconductors, artificial intelligence, and biotech, they have also built the Chinese Communist regulatory model for the tech industry and its use of users' data. In some ways going further than the United States, Europe, and other jurisdictions' regulators in tackling online privacy issues, it is important to note that the Chinese leadership is less concerned about individual users' protections and more about the control of data and information outside CCP control.

Simply put, China's approach towards data is that only the party can spy on you—not only to achieve the CCP's goals of internal control, surveillance, and censorship, but also to ensure that no entity beside the party has a comprehensive picture of what is going on in China. From business data and stats on transactions to the ride share and food ordering habits, the CCP continues to expand its definition of what data is sensitive or related to national security. Just as it is applied to conventional industries and, increasingly, financial data, so too does China's digital data.

Beijing's regulatory bodies, mainly the Cybersecurity Administration of China, have been cracking down on tech companies listing overseas and their data management practices. The most notable example in 2021 was Didi Chuxing, the "Uber of China", where Chinese regulators forced a delisting of that company's U.S. initial public offering (IPO). While one of Didi's "sins" was the rush to IPO overseas despite Beijing's qualms, another was that Didi was specifically tracking the rideshare journeys of government officials as part of their data operations.

Again, for the Chinese Communist Party, the concern is not so much the gathering of the data, but who controls and sees the "data dashboards". Didi can tell Beijing much about how its citizens are traveling, while AntPay can deliver the details on their financial health. Combined with facial recognition technologies, tracking of telecom and social media communications, and other tools, Beijing is building its data-driven panopticon. Companies from overseas must meet its standards to do business in the Chinese market, while it exports the technical foundation of this to other despots, and hacks foreign networks for the other data needed to learn about overseas individuals—e.g. how the hacking of the U.S. government Office of Personnel Management and the user records of hotels and airlines can help to penetrate potential U.S. intelligence cover identities or identify other targets for Chinese espionage.

In China, control of data is less about users' privacy and more about the party's capacity for internal control, planned economy, and control of digital society. What developed during the COVID-19 pandemic was the ultimate expression of China's model of digital repression.

The Pandemic & China's Digital Repression Model

Before the pandemic, there was already a greater understanding of how China employed digital surveillance, censorship, and control. Stories from Xinjiang about the genocide of the Uyghur population illustrated how a range of tools were used to surveil and identify those targeted for re-education, imprisonment, or execution. Others told of how online postings were controlled and censored to make sure that criticism of the regime was scrubbed from online forums. Still more explained how new technologies were being rolled out to create smart surveillance systems building on other smart city infrastructure. Again, the inherent technologies were not good nor bad; artificial intelligence, facial recognition, networked cameras, and other technologies are all useful, but the model in which the CCP was combining them created a perfect marriage of cyberspace censorship, networked surveillance, and real-world detention—or worse.

What developed during China's COVID lockdowns represented the inevitable conclusion of combining these technologies of digital censorship and repression, tracking of COVID "testing passports" or "health codes", and a real-world physical infrastructure of lockdowns and quarantine detention. These digital tools went far beyond some of the ones employed in the United States and other countries for contact tracing and notifying users of potential exposure to infection. Analysis of the underlying code of one of the Alipay health apps created by Alibaba subsidiary Ant Financial would automatically share user data including location with police as soon as they activated the app. Combined with the assignment of a red, yellow, or green health code determined not only by test results but also the algorithmic predictions provided by data from the users' device, the user was subject to various restrictions in travel or possible quarantine at home or detention facility.[5]

[5] Paul Mozur, Raymond Zhong and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." *The New York Times.* March 1, 2020, accessed February 17, 2023. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Reports from China demonstrated how the underlying control codes in the health apps could be manipulated to control public gatherings and to impose other forms of internal control. In Zhengzhou, China, authorities used health code apps to issue “red codes” to restrict the gathering of otherwise healthy people who had grievances against local officials. Checkpoints used to check COVID status were also employed to check Chinese citizens’ phones for software that might allow for encrypted messaging or access to virtual private networks (VPNs) that allowed users to avoid government monitoring or “Great Firewall” internet blockages.[6]

Ultimately, Chinese citizens’ frustrations with COVID lockdowns and the resulting economic disruption—as well as other grievances with the CCP and Xi Jinping’s consolidation of power—boiled over, resulting in widespread protests. Starting in November 2022, protests spread throughout Chinese cities, with leaders ultimately moving to relax COVID restrictions. This was not a reaction to protests, as Xi Jinping was ultimately responding to pressure from corporate leaders who warned that continued lockdowns threatened the foundation of China’s economy and its role as a global factory and the basis of critical supply chains.[7]

The protestors, in fact, would find themselves facing the long reach of China’s digital surveillance and the resulting crackdown on the public display of dissent. Those who participated in the protest were identified by social media postings as well as video surveillance, cell phone tracking, and other tools employed by the CCP for internal surveillance. Some were detained by authorities, facing lengthy interrogations and strip searches, while others noticed deeper physical and digital surveillance. Using a long-time technique of the Chinese authorities, parents and other family members were also notified that their children or relatives had engaged in protests and could be subject to surveillance and detention—raising the stakes for the entire family. Reports from those detained and the scale of the repression suggest that the mass surveillance of entire districts’ cell phone towers, other devices, and facial recognition are driving most of the regime’s efforts to crackdown on protest participants and determine whether there were any leaders to what appeared to be a largely organic and decentralized display of frustration.[8]

[6] Wen Dong & Liam Scott, “COVID Controls Offer Insight Into China's Surveillance Network.” *Voice of America*. December 29, 2022, accessed February 17, 2023. https://www.voanews.com/a/covid-controls-offer-insight-into-china-s-surveillance-network/6888440.html

[7] Keith Zhai & Yang Jie, “Letter from Apple Supplier Foxconn’s Founder Prodded China to Ease Zero-Covid Rules.” *The Wall Street Journal*. December 8, 2022, accessed February 19, 2023. https://www.wsj.com/articles/letter-from-top-apple-supplier-foxconn-prodded-china-to-ease-zero-covid-rules-11670504366

[8] Cate Cadell & Christian Shepherd, “Tracked, detained, vilified: How China throttled anti-covid protests.” *The Washington Post*. January 4, 2023, accessed January 6, 2023. https://www.washingtonpost.com/world/2023/01/04/china-surveillance-protests-security/

That China also seeks to export its surveillance model around the world is well understood. The export of specific surveillance technologies and systems is one aspect of this. So too, is the proliferation of hardware, software, and apps from China that work to harvest data from overseas. This overseas harvesting of data can be used for China's own development of artificial intelligence and machine learning models, as well as to create the data pools helpful for foreign and internal espionage and surveillance.

In the United States and many other like-minded countries, there is the realization of the challenge to digital freedom posed by hardware or software that could ultimately used by the Chinese Communist Party to steal or to manipulate data. Still, the developing world, the broader "Global South" sees less of a distinction between the U.S.-and-allied-led and CCP-led models, as they believe that all the actors engage in some form of surveillance. Therefore, it is important to illustrate the distinction between our models; to focus on how the difference between how the models empower or repress digital citizens; and to build aid and investment models (plurilateral/multilateral agreements and public-private partnerships) that work across the globe building collaboration with local partners to strengthen digital infrastructure and digital development.

Russia's Post-Ukraine Digital Repression

Following Russia's expanded invasion of Ukraine, two parallel trends continued to shape Moscow's use of the digital environment. First, within Russia itself, the Kremlin sought to further tighten its control over the information space, circumscribing the use of foreign apps, sharply limiting the ability of citizens to access foreign sources of information, and promote its own domestic propaganda. Second, the Kremlin continued its overseas efforts to undermine Western narratives, conduct political warfare, and attempt to sow division and discord within the United States and Europe, whilst at the same time working to keep the rest of the world, if not on its side, then wholly neutral.

Moscow has steadily worked to create its own sovereign internet[9], cutting the country off from the rest of the world. Here, in May 2019, Putin signed legislation that closed Russians off from information that contradicted the Kremlin's narrative. Often seen as the "sovereign internet law" it was, in fact, a series of amendments to existing law that mandated the installation of technical means to control the flow of information, centralize network management, and establish a Russian Domain Name System.[10] According to the German Council on Foreign Relations, this had three specific goals: creating a mechanism for Internet surveillance within Russia, establish the state as the central regulator of the Internet, and expand its model of state-control of the Internet abroad.

Most recently, the Kremlin banned government officials from using popular messaging apps including Discord, Microsoft Teams, Skype for Business, Snapchat, Telegram, Threema, Viber, WhatsApp and WeChat.[11] The ban on Telegram is interesting, as it is one of the more popular and widely used messaging platforms across Russia and by Russians fighting in Ukraine, despite it being formally banned in 2018 for failing to handover encryption keys to the FSB.[12] Arguably, this crackdown on official use of these services is likely an attempt to limit the flow of information across non-state-controlled information platforms from Ukraine. The United States and United Kingdom, in particular, have demonstrated surprising awareness of Russian plans and intentions.

[9] Andrei Soldatov & Irina Borogan, "The New Iron Curtain Part 4: Russia's Sovereign Internet Takes Root." *CEPA*. April 5, 2022. https://cepa.org/article/the-new-iron-curtain-part-4-russias-sovereign-internet-takes-root/

[10] Alena Epifanova, "Deciphering Russia's 'Sovereign Internet Law.'" *DGAP*. January 16, 2020. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

[11] Phil Muncaster, "Russian Government Bans Foreign Messaging Apps." *Info Security*. March 2, 2023. https://www.infosecurity-magazine.com/news/russian-government-bans-foreign/

[12] Phil Muncaster, "Telegram App Banned in Russia." *Info Security*. April 16, 2018. https://www.infosecurity-magazine.com/news/telegram-app-banned-in-russia/

This also fits within Russia's broader attempts to assert control over the media space, and in particular digital outlets. While most of Russia continues to consume state-backed or state-run television propaganda this has been, according to the Levada Center, been steadily declining.[13] Moreover, younger Russians increasingly get their news and information online. In October 2022, the Kremlin declared Meta to be an extremist organization, banning its activities in the country.[14] Facebook and Instagram, owned by Meta, were in March of the same year banned for "Russophobia".

The remaining accessible Internet within Russia is highly sanitized, dominated by state media, and leaving few opportunities for Russians interested in or inclined to connect with the outside world.[15]

While circumvention technologies such as VPNs are enjoying increasingly widespread use and there is an appetite within the country for foreign news about the war, the Kremlin will continue to assert its control over the social media and information space to stifled dissent and control the narrative about its "special military operation".

Propaganda & Information Control

It is also important to recognize that Russia's traditional and virtual propaganda is as often, if not more so, targeted at its own citizens and non-Western targets (discussed below). The West's understanding of Russian information warfare has markedly improved since Moscow's expanded invasion of Ukraine, but it has almost over-corrected, assuming that it is all about the West. In fact, the much parodied "Z" and other attempts at marshalling support for Russia's invasion is much more about its own citizens as well as creating muddy waters in which Russian-sympathizers can swim. This is, of course, part of Russia's long-game in Ukraine: it hopes to undermine the West's political support for Kyiv by exploiting existing divisions, fomenting new ones, and using a "firehose of falsehood" to overwhelm the West.[16]

More broadly, by severely constraining and limiting the information to which Russia's citizens are exposed, punishing anyone critical of the war, and by flooding the remaining information

[13] Sergey Davydov, "How the war changed Russia's media consumption." *Riddle*. November 18, 2022. https://ridl.io/how-the-war-changed-russia-s-media-consumption/

[14] Joe Tidy, "Russia confirms Meta's designation as extremist." *BBC*. October 11, 2022. https://www.bbc.com/news/technology-63218095

[15] Allie Funk, "Digital Repression is Deepening, But Civil Society Wins Give Reason for Optimism." *Freedom House*. October 20, 2022. https://freedomhouse.org/article/digital-repression-deepening-civil-society-wins-give-reason-optimism

[16] Christopher Paul & Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model." *Rand*. 2016. https://www.rand.org/pubs/perspectives/PE198.html

space within the country, the Kremlin is hoping to stave off any potential opposition to its activities. This does, of course, not mean that all Russia's support the war, and that is not necessarily the Kremlin's objective. Rather, it is sufficient to keep its citizens on the sidelines, disengaged, disconnected, and disinterested in the war. An apathetic citizenry is a compliant citizenry, or at least a manageable one, when and if domestic conditions appreciably deteriorate.

Russia's digital repression is a mirror of its real-world repression. Russia's 2012 "foreign agent" law sharply curtailed the ability of journalists, opposition figures, and human rights groups to operate within the country. In July 2022, Putin expanded the law, which previously required prosecutors to demonstrate that an individual had received financial or material support from a foreign source, to target any activities that "contradict the national interests of the Russian Federation."[17] On 4 March, 2022, Putin signed into law a measure that criminalized objective reporting of the war in Ukraine.[18] This forced many of the remaining independent journalists and outlets out of the country, or risk facing up to 15 years in prison.

Putin's increasingly assertive control over this space is a marked change, in some degrees from prior to the war. The Kremlin was both attune to and needed the public's support, even if it was manufactured and highly circumscribed. Appearances matter as did the public's opinion. While the opposition was, largely, tame, it still existed and was part of the pantomime political process that was legitimating for Putin and his presidency. Indeed, expert Mark Galeotti has described it as "late-stage Putinism" and more akin to the latter years of the Brezhnev era.[19] This period was marked by crackdowns on the opposition and a closing of the limited open spaces within the Russian information sphere.

The likelihood that this pattern of behavior continues is significant. It is clear that Russia's "special military operation" in Ukraine has not gone the way he and his advisors expected. The Ukrainian Armed Forces have performed far better than expected, the Western alliance has provided much greater sustained aid than anticipated, and the performance of Russia's military has been shockingly poor. February 2023 marked the first anniversary of the war, and there is little to suspect that it will be resolved within the next year. The battle lines will certainly change, and Russia will likely find itself increasingly on the backfoot as Western aid including main battle tanks reaches the front, but a pathway to a cease-fire or end to the war is, as of this

[17] RFE/RL's Russian Service, "Putin Signs Off On Harsher 'Foreign Agent' Law." Radio Free Europe/Radio Liberty. July 14, 2022. https://www.rferl.org/a/putin-signs-off-harsher-foreign-agent-law/31943645.html

[18] "Russia's Crackdown on Independent Media and Access to Information Online." *CSIS*. March 30, 2022. https://www.csis.org/analysis/russias-crackdown-independent-media-and-access-information-online

[19] Mark Galeotti, "Why this is the beginning of the end for Vladimir Putin." *The Telegraph*. February 25, 2022. https://www.telegraph.co.uk/news/2022/02/25/beginning-end-vladimir-putin/

writing, unclear. Russia's poor performance led to a partial mobilization in September 2022[20], and there is speculation that a second mobilization may be necessary.[21]

The longer that this conflict continues and the worse Russia performs, the greater the Kremlin needs to control information at home. Sharply limiting domestic access to foreign news sources, proscribing media outlets, banning foreign communications apps, and flooding the remaining space with Russian propaganda will become the norm, rather than the exception. Whereas the regime tolerated some dissent and some loyal opposition, anything that undermines the Kremlin's narrative at home will almost certainly be forbidden.

The Narrative & Information War

This then turns to the second key factor of Russian digital repression, which is almost, arguably, a form of positive repression, not in a value driven sense, but in the Kremlin's efforts to advance its own narrative in the information war. For the West, the information war is over—there is unanimity, in the West's mind, against Russia's invasion and concomitantly, unanimity in support for Ukraine. The West has, however, won the war against itself and sees only the information it wants to see.

By contrast, Russia has worked aggressive in Latin and South America, Africa, and the Middle East—rather awkwardly and perhaps inaccurately termed the "Global South"—to undermine Western narratives, advances its own propaganda, and achieve neutrality at worst or support at best for Moscow. South Africa, for example, recently held naval drills with Russia and China.[22] Across the Africa, Russia has worked assiduously to court countries in Africa for both narrow commercial interests, but also diplomatic support, whilst undermining Western reach.[23] Indeed, Russia's success at driving French forces out of Burkina Faso is indicative of this effort.[24] Thus far,

[20] Mary Ilyushina & Annabelle Timsit, "What does Putin's partial military mobilization mean for Russia and Ukraine?" *Washington Post*. September 21, 2022. https://www.washingtonpost.com/world/2022/09/21/russia-partial-mobilization-putin-war-ukraine/

[21] Politico, "As second mobilization looms, Russian men are staying put (for now)." *Politico*. February 4, 2023 https://www.politico.eu/article/second-mobilization-russia-men-vladimir-putin-ukraine-war/

[22] Kate Bartlett, "South Africa joins Russia and China in naval exercises." *NPR*. February 18, 2023. https://www.npr.org/2023/02/18/1158169215/south-africa-joins-russia-and-china-in-naval-exercises

[23] Clara Ferreira Marques, "Is Russia Winning the Battle For African Support?" Washington Post. July 29, 2022. https://www.washingtonpost.com/business/energy/is-russia-winning-the-battlefor-african-support/2022/07/29/6d950734-0efb-11ed-88e8-c58dc3dbaee2_story.html

[24] Laura Kayali & Clea Caulcutt, "How Moscow chased France out of Africa." *Politico*. February 23, 2023. https://www.politico.eu/article/france-africa-russia-emmanuel-macron-vladimir-putin-mali-central-african-republic-burkina-faso/

countries in Latin and South America have also refused requests to provide arms and munitions to Ukraine.[25]

This is a blind spot in the West's understanding of the information war and this form of positive digital repression. Pro-Kremlin narratives are, rightly, condemned on Western social media, supporters are called out and criticized, and Russian propaganda by proxy exposed. Yet, while the West criticizes this propaganda, it misses the fact that it is in many cases not designed for or intended for Western consumption—first and foremost it is for Russian audiences (as noted above), but equally as important it is meant for non-aligned, non-Western targets. A recent study by the Atlantic Council's Digital Forensic Research Lab found 56 channels on Telegram divided into three networks spreading pro-Kremlin propaganda in Europe, Asia, South America, and the Middle East.[26]

Both at home and abroad, as the "special military operation" continues, Russia will need to increase its digital repression, both to limit what its own citizens sees, and to shape the views of other countries. Putin is banking on the breaking of the West's political resolve, and whilst that may not happen in the near term, the absence of global support for sanctions, embargoes, and other measures intended to isolate Russia—or the erosion of existing restrictions—will undermine the efficacy of these efforts.

[25] Michael Stott, Christine Murray, Lucinda Elliott, Carolina Ingizza and Guy Chazan, "'We are for peace': Latin America rejects pleas to send weapons to Ukraine." *Financial Times*. February 15, 2023. https://www.ft.com/content/fc8d51c8-5202-4862-a653-87d1603deded

[26] Sayyara Mammadova & Nika Aleksejeva, "Networks of pro-Kremlin Telegram channels spread disinformation at a global scale." *DFRLab*. March 1, 2023. https://medium.com/dfrlab/networks-of-pro-kremlin-telegram-channels-spread-disinformation-at-a-global-scale-af4e319bd51e

The U.S. Digital Freedom Debate

While China and Russia have continued to move ahead with their models of digital repression, U.S. policymakers are debating many of the issues related to digital freedom—both at home and abroad. Much of the domestic debate has centered around the power of "big tech" companies and platforms, but there is little in the way of agreement on solutions given the partisan deadlock on Capitol Hill. At the same time, the administration's domestic regulatory approach has looked more towards consolidation in the tech industry.

In terms of the digital freedom debate in the United States and the underlying questions of citizens' trust in digital society, much of the U.S. debate quickly moves to content moderation and countering disinformation—where political polarization complicates the legislative proposals and protections for speech and civil rights limit what government can do. While the debate about content moderation breaks along partisan fault lines, discussions over data management and user privacy are more complicated, as U.S. federal-level legislation stalls and state-led efforts move forward.

Where U.S. policymakers have found the most consensus is the area of digital infrastructure protection and security. While not traditionally included in most debates over digital freedom, this is important to ensure that Americans can trust the infrastructure for their digital lives, while also ensuring that the information they see is accurate and their data is protected.

What becomes critical in these debates is the example that the United States sets in a global competition to set tech standards and the future digital "rules of the road." Beyond the debates underway by policymakers, the U.S. system also gives platforms themselves significant leeway for private sector platforms to moderate their own content, set standards, and harvest user data. Still, these firms can also use their size and influence to shape industry behaviors and best practices, as well as consumer expectations. As policymakers consider their approach to the U.S. tech industry, they must strike a careful balance between thoughtful regulation of industry and understanding the competitive power of these firms in a global struggle for the digital future.

Content Moderation

Debates over content moderation largely break along partisan lines—with concern over disinformation, but seeing the other party as the bad actor. When platforms remove conspiracy theories or disinformation aligned against one's political view, that's "content moderation", but when one's own views come into question, that quickly becomes "censorship."

Agreeing with or believing in disinformation or conspiracy theory does not make it reality, but for those who do, any effort to counter that disinformation quickly becomes "censorship of the 'truth'." One lightning rod in the debate over platform regulation is "Section 230". Considered by many to be vital to how the modern internet works, Section 230—referring to Section 230 of the 1996 Communications Decency Act, places responsibility for content posted online in the hands of the individual(s) posting it, rather than the platform upon which it is posted.

Each side has targeted Section 230, decrying it when they wish to hold social media platforms or other content sites responsible for what is posted. However, a recurring problem is that there is no consensus on what, if anything, could replace Section 230. Furthermore, many believe that there is nothing wrong with how Section 230 currently works, and that alternative models open the door to greater censorship, greater litigiousness, further splintering of the internet, or, worse yet, all of the above.

The future of Section 230 may rest outside the hands of legislators at this point, as the U.S. Supreme Court considers the arguments laid forth in *Gonzalez v. Google*, on February 21, 2023. The case questions whether Alphabet/Google, owner of YouTube, can be held responsible for ISIS recruiting videos that led to the 2015 Paris terrorist attack in which the daughter of Reynaldo Gonzalez was killed. Analysis of arguments suggests that the Justices seemed reticent to issue a broad ruling significantly reshaping of the rule, but the outcome is uncertain until they deliver the ruling.[27] It was Justice Kagan who gave some levity to the proceedings when she declared the Supreme Court Justices were "not, like, the nine greatest experts on the internet."

If the Supreme Court does come back with a ruling that requires some form of legislative response or fix, the lack of a consensus and a growing chorus against the current form of Section 230 makes it unlikely that there will be a quick or easy solution. Current political dynamics make it unlikely for any significant legislative pushes before sometime after the 2024 election.

Still, despite a lack of legislative action, there is also growing discussion about how various key social media platforms are approaching content moderation given changes in management priorities. These questions about content moderation become more urgent, given concerns about 2024 electoral interference, as well as how technology like artificial intelligence and "deepfake" technology can create highly-convincing disinformation—while already being used for sexual abuse and blackmail.

[27] Amy Howe, "'Not, like, the nine greatest experts on the internet': Justices seem leery of broad ruling on Section 230." *SCOTUSBlog*. February 21, 2023, accessed February 24, 2023. https://www.scotusblog.com/2023/02/not-like-the-nine-greatest-experts-on-the-internet-justices-seem-leery-of-broad-ruling-on-section-230/

While legislative efforts stall, the private sector still plays a significant role in content moderation, both in the standards set by the platforms and their enforcement. However, these private sector efforts can be affected by changes in management priorities or re-allocation of resources. Meta, parent of Facebook and Instagram, has been criticized for emphasizing the shift to the virtual/augmented reality "Metaverse", and thus de-emphasizing content moderation. Critics say this is seen in the firings of content moderators, as well as the closure, due to lawsuits and worker unrest, of subcontractors who moderate content for Facebook.[28] As part of a broader restructuring under the leadership of Elon Musk, Twitter has also made cuts to staff responsible for misinformation and accounts posted by state media entities.[29] Finally, as part of broader critiques of TikTok, questions have been repeatedly raised about how the app determines, via algorithm, what users see, as well as how the platform may or may not censor content related to topics that are sensitive to the Chinese Communist Party.

These controversies surrounding private sector platforms, and the difficulty in reaching any legislative consensus on a response, suggests that the solution will likely be found in a combination of better corporate best-practices and user education to improve digital literacy. Furthermore, courts may strike down government content moderation efforts under the First Amendment, while other efforts will likely become politicized between the party in power and that in opposition. Finally, government-led efforts should always be approached with caution, given that assumptions about one party or "your side" being in control can always be upended—then your opponent can have the same tools of moderation, and censorship, that you once wielded.

Therefore, platforms should strive for transparency so that users can more easily understand the rules for posting content as well as why—in basic terms that do not necessarily disclose proprietary information—the platforms' varying algorithms show them the content they see. These terms and conditions should also be clear that there is a difference between legitimate political speech and debate, and calls for violence, sexual abuse, and many of the other "trolling" behaviors that plague social media users.

[28] Casey Newton, "Another Facebook content moderation company quits the business." *Platformer*. January 10, 2023, accessed February 2, 2023. https://www.platformer.news/p/another-facebook-content-moderation and Malea Martin & Cameron Rebosio, "Terminated Meta content moderators worry about fake news flourishing in their absence." *Pleasanton Weekly*. January 28, 2023, accessed February 2, 2023. https://www.pleasantonweekly.com/news/2023/01/28/terminated-meta-content-moderators-worry-about-fake-news-flourishing-in-their-absence

[29] Davey Alba & Kurt Wagner, "Twitter Cuts More Staff Overseeing Global Content Moderation." *Bloomberg.* January 7, 2023, accessed February 2, 2023. https://www.bloomberg.com/news/articles/2023-01-07/elon-musk-cuts-more-twitter-staff-overseeing-content-moderation

Privacy & Data Management

While there are debates about privacy protections, there has been a lack of federal action within the United States. The most significant action has been taken at the state level by the States of California, Colorado, Connecticut, and Utah, and the Commonwealth of Virginia who have all implemented their own privacy legislation. Other states are considering a model, based on legislation introduced in the U.S. House.[30] In the absence of this federal legislation, however state-by-state legislation raises concerns over a patchwork of regulation—or a circumstance where a few large states dictate *de facto* regulation for the country. Even if large states do not dictate terms, a patchwork where platforms must meet fifty-plus varying regulatory regimes would greatly increase the burden on firms. Large incumbents would have the resources to handle such an environment, but it would become more difficult for startups to grow to national size. This would also harm the unified, but diverse data pool, that the United States offers companies working to build data models and train artificial intelligence and machine learning.

While legislative proposals have been put forward, some based on the European GDPR model or the California model, there has not been consensus to move ahead with any one proposal. Additionally, the state-level legislation complicates any compromise at the federal level. Federal-level legislation would preempt any by the states, so lawmakers from states that have more stringent privacy protections and data management regulations than any proposed federal compromise bill would likely face pressure to thwart any such bill. A national data privacy bill passed the House Commerce Committee with bipartisan support in 2022, but Speaker Nancy Pelosi (D-CA) refused to bring it to the House floor for a vote for the reason mentioned above. It remains to be seen whether this legislation will advance in the current Congress.

Again, given the stalled legislative process, attention moves to the platforms themselves and what existing authorities can be used by regulators. Twitter was already under FTC consent decrees related to past violations of users' privacy protections, and investigations have been deepened in March 2023.[31]

TikTok, given concerns about its Chinese ownership under ByteDance, faces the gravest concerns from policymakers about privacy and data management. During the Trump administration, efforts began to create a separate U.S. infrastructure for U.S. TikTok users' data, while also aiming to learn more about what user data could be transmitted back to China, as

[30] Alfred Ng, "The raucous battle over Americans' online privacy is landing on states." *POLITICO.* February 22, 2023. https://www.politico.com/news/2023/02/22/statehouses-privacy-law-cybersecurity-00083775

[31] Kate Conger, Ryan Mac, & David McCabe, "F.T.C. Intensifies Investigation of Twitter's Privacy Practices." *The New York Times*. March 7, 2023. https://www.nytimes.com/2023/03/07/technology/ftc-twitter-investigation-privacy.html

well as how the platform may be used to steer information, propaganda, or disinformation to users. The most recent controversy has been whether the platform is being used to steer content opposing a controversial oil project to be opened in the Alaskan arctic.[32]

Through this debate, a consensus is growing among policymakers to ban TikTok in the United States. However, what this exactly means depends on the various proposals. The consensus seems to be moving towards legislation that would authorize President Biden to ban TikTok or create a process for an administration to investigate and respond to companies that have access to U.S. users' data and present potential national security risks. The "Deterring America's Technological Adversaries Act" or DATA Act, passed from the U.S. House Foreign Affairs Committee, led by Chairman Michael McCaul (R-TX), is extremely broad.[33] It directs the president to sanction entities should they carry out any activities on behalf of China, under China's influence, or contributing to China's national security, intelligence, censorship, algorithmic development, or malicious cyber campaigns, alongside any other threats to or electoral interference in the United States or other allies.

Senator Mark Warner (D-VA) has introduced the ''Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act'' or RESTRICT Act. This would create a more procedural approach, but would still grant the President and Secretary of Commerce the broad authority to "deter, disrupt, prevent, prohibit, investigate, or otherwise mitigate" national security threats coming from services that have access to the "sensitive personal data" of more than 1 million Americans.[34]

Many of the concerns about digital freedom, user privacy, content moderation, and geopolitical competition came together in the March 23, 2023, hearings of the U.S. House Energy & Commerce Committee featuring the testimony of Shou Zi Chew.[35] Through the contentious questioning what became clear was that while TikTok does engage in many of the same activities of other social media and digital apps, TikTok must be banned because of: TikTok's Chinese parent company ByteDance; its ties to the Chinese government and Chinese Communist Party; Beijing's control over the private sector; and Chinese regulations controlling and preventing export the algorithm powering TikTok. Embodied within the debate over TikTok are not only questions about the competition for digital and technological leadership but also

[32] Grace Conley & Esme Stallard, "TikTokers target controversial Willow oil project." *BBC News*. March 11, 2023. https://www.bbc.com/news/science-environment-64906323

[33] https://docs.house.gov/meetings/FA/FA00/20230228/115363/BILLS-118HR1153ih.pdf

[34] https://www.warner.senate.gov/public/_cache/files/3/f/3f2eaae6-09ad-49e1-b254-46289cf20cca/843D73B1823EA0D4122B4365262410D6.restrict-act-final-text.pdf

[35] "TikTok CEO Testifies at House Commerce Committee." C-SPAN. March 23, 2023. https://www.c-span.org/video/?526609-1/tiktok-ceo-testifies-house-commerce-committee

how we want to shape our own digital society. Banning TikTok or even more broadly restricting data flows to countries of concern will not address content moderation, users' mental health, algorithmic recommendations, or many of the other concerns raised during the hearing. Lawmakers need to carefully consider the precedents they will set, the global standard that might be created by U.S. actions, and the response from the American and global public to what is an extremely popular platform.

At the same time and despite the statements from lawmakers and the legislative push underway, many users are indifferent to the concerns raised by privacy experts, or acknowledge that they are being spied upon but see it as simply a part, or indignity, of modern life. Users also acknowledge that many other platforms do it, save for those who charge extra for privacy protections.[36] Additionally, many of the concerns about user data and privacy steered towards platforms ignore the broader "data broker" market in the United States where many existing databases of ostensibly anonymized user or customer data are available for purchase by anyone from investigators to journalists to stalkers. Even if anonymized, overlapping databases can still be utilized to unmask an individual, or individuals, and anything ranging from their whereabouts to personal preferences.

Despite the increasing cynicism displayed by the user base and the absence of legislative consensus, there is an opportunity. In a society that understands the basis of the digital economy—i.e. if the platform is free, you're the product—then we can begin to build a more transparent understanding of data management and the value of our own data. During CSPC discussions with stakeholders, it was repeatedly suggested that platforms could collectively adopt some form of "Nutrition Facts" or similar, simply-understood labeling that could at least accompany the byzantine terms and conditions that few users read, then users could make more informed choices.

Protecting Digital Infrastructure

Where there has been the greatest consensus among U.S. policymakers is the protection of U.S. digital infrastructure. While this has largely been focused on physical infrastructure, controversies over TikTok have lawmakers increasingly looking at how the platforms themselves fit into concerns about digital security. This consensus on securing digital infrastructure—both hardware and software—is essential for digital freedom because it ensures that citizens can trust the information they see and that their increasingly networked lives will not be disrupted

[36] Natalie Sherman, "TikTok users shrug at China fears: 'It's hard to care'." *BBC News.* March 10, 2023. https://www.bbc.com/news/business-64827885

by bad actors. These efforts by lawmakers aim to reduce the threat of untrustworthy equipment in our digital infrastructure, promote greater vendor diversity, ensure digital resilience, and "bake-in" security into future digital technology, as well as improving our own digital behavior.

Over the past decade, the most visible effort was the push back from the United States and allied governments against the Chinese telecom firms Huawei and ZTE. These efforts have expanded to include a range of Chinese firms involved in technologies like AI, facial recognition, telecoms, cameras, drones, and other technologies of concern. The United States and other allies moved to ban these companies, and in the United States, the 2021 Secure Equipment Act of 2021 broadened the FCC's authority to restrict technology from companies on the FCC's "covered list" of national security threats. The FCC's program to "Rip and Replace" ZTE and Huawei equipment will also require further appropriations from lawmakers, as demand for reimbursement to replace the untrustworthy equipment has surpassed the $1.9 billion original allocation by more than $3 billion.[37]

Lawmakers' efforts to secure infrastructure are also combining with efforts to promote vendor diversity and lower the digital divide in the United States. The rollout of 5G networks and future 6G networks presents an opportunity for further investment and deployment of Open RAN (ORAN) technology. Commitments by the United States and key allies, such as Japan, to Open RAN technology, as well as accelerated pilot programs, can foster more rapid commercial adoption of the technology. Already providers like Dish and Rakuten are deploying ORAN technology, and further developments in ORAN technology will allow for greater vendor diversity and more flexibility in deploying 5G and 6G networks. Building a strong ORAN industry, both in R&D and commercial vendors, will help to ensure continued telecom innovation leadership in the United States and allied countries.

These efforts to protect U.S. infrastructure make clear U.S. priorities for digital security, while also sending a signal to allies, partners, and the private sector about the seriousness with which we take the threats to digital freedom. As these programs are planned and carried out at the domestic level, they can also be better coordinated with global efforts, as will be discussed in the following section.

Finally, any effort to ensure digital security requires an educated population. Digital literacy and digital citizenship efforts will not be a panacea, but they are a critical path towards addressing the human element of digital security. The basics of "cyber hygiene" can go a long way towards

[37] Senator Cynthia Lummis, "US must fully fund 'rip and replace' of Huawei, ZTE telecom equipment." *The Hill*. February 23, 2023, accessed March 8, 2023. https://thehill.com/homenews/3863539-us-must-fully-fund-rip-and-replace-of-huawei-zte-telecom-equipment/

also addressing many of the threats to digital freedom—be it cybersecurity or greater awareness of disinformation. Generational cyber savvy is also important, but the aspects of digital citizenship must be emphasized alongside cybersecurity. While we can operate networks on “zero trust” to ensure security, we cannot operate a democracy that way—digitally or physically.

Opportunities for Global Cooperation

Given the global nature of this competition, it is vital that the United States work with allies and partners on advancing a common digital freedom agenda. A significant challenge in this effort will be that not all our partners, and even some allies, have differing approaches to digital freedom, and some could be rightfully accused of behavior more in line with that of digital authoritarians.

While continuing to advocate for digital freedom and ideally leading by example, the United States will find itself also having to move forward with a selective international agenda—and aim to seek consensus where possible alongside allies. This agenda needs prioritization based on where priorities overlap and what is feasible. The strategy should take into account that many nations do not want to be forced to choose between the "U.S. model" or the "China model", and at the same time, that a splintering of the internet has negative economic and social implications. Elements of successful strategy are a) Making the digital freedom model relevant and appealing; b) Leveraging existing institutions and opportunities; and c) Boosting program funding.

Making the Digital Freedom Model Relevant & Appealing

Here it will also be important to get the message right. We need to explain the benefits to the *economy* (fosters innovation, entrepreneurship, job creation, and broad-based economic growth) and *society* (engenders stronger social compact, equity, and inclusion) of the Western-led model. Together, these two forces – economic and societal benefits - lead to more resilient societies. At the same time, we must be forthcoming about the hazards of an open internet (disinformation, polarization, protection of minors online, etc.) and share best tools to address them, allowing for policy space for countries to implement their own appropriate guardrails. We also need to explain how the various pillars— connectivity, open data for public benefit, data flows with trust, security, and the multistakeholder approach— work together to achieve desired economic and societal outcomes.

On open data, the U.S.-Mexico-Canada regional trade agreement (USMCA) notes that facilitating public access to and use of government information fosters economic and social development, competitiveness, and innovation. As many consider Washington and Beijing equally guilty of espionage and U.S. and Chinese firms equally rapacious for users' data, it will be important to emphasize how matters like the rule of law, due process, limits on government data collection, transparency, and accountability protect civil liberties in the open internet model, while also enhancing partner nations' digital development and opportunities for growth. It will also be important to emphasize the tradeoffs that come with choosing the Chinese option—similar to those tradeoffs for physical infrastructure. Open networks do not mean unsecure networks. Nor do they mean relinquishing sovereignty: governments can still choose how they will safeguard their national security and protect consumers/citizens (including data privacy) and preserve open competition in the digital economy (including regulating platforms or "over the top" digital service providers)—as long as these polices ensure non-discriminatory treatment and that any restrictions on data flows are necessary and proportionate. These principles are enshrined in the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). They also appear in the USMCA regional trade agreement chapter on Digital Trade.[38]

Foster Cooperation to Advance a Digital Freedom Agenda

Here, upcoming events like the upcoming G-7 summit led by Japan and other meetings between U.S., Western Hemisphere, European, Japanese, and other like-minded leaders should emphasize opportunities for convergence on areas of existing agreement. Given that over half of all global data flows move across the Atlantic, convergence between U.S. and EU digital standards would be significantly helpful to the global digital freedom agenda. The U.S. and EU have agreed on a data flows framework to replace the U.S.-EU Privacy Shield, although this arrangement may still be subject to court challenge in the EU. At the same time, the EU's new regulations on digital platforms and service providers, known as digital services act (DSA) and digital markets act (DMA), have widened the gap between the U.S. and EU regulatory frameworks.[39] U.S. and EU Trade and Technology Council represents an opportunity to jointly advance the digital trade agenda, including norms and standards.

The OECD is another useful forum for collaboration and standard setting: it has produced digital policy standards and norms to guide a country's digital transformation in areas like broadband connectivity, artificial intelligence, children in the digital environment, enhancing access to and sharing of data, digital security, protection of privacy, and transborder flows of personal data.[40] It is important to reach solutions in transatlantic, transpacific, or G-7 forums to present a more united front on digital issues to the world. Similarly, as evidenced by recent U.S. and Japanese victories in elections to the ITU, leadership in the global bodies that set telecommunications and digital standards will be important to ensure that the future model for the internet is driven by innovators and empowered digital citizens rather than governments. Over 60 countries signed

[38] Office of the U.S. Trade Representative, "USMCA: Chapter 19, Digital Trade." Accessed March 24, 2023. https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

[39] European Commission, "The Digital Services Act package." Accessed March 24, 2023. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[40] OECD Database of Legal Instruments https://legalinstruments.oecd.org/en/instruments

the Declaration for the future of the internet in 2022.[41] This declaration provides a platform and opportunity for advancement of digital freedom principles. The Freedom Online Coalition was established in 2011 and comprises thirty-five member countries committed to advancing Internet freedom and human rights online.[42]

The 2023 Democracy Summit taking place in Washington, DC will include a U.S. government-hosted event on "Advancing Technology for Democracy".[43] Policymakers should look into combining some of these multilateral initiatives and refreshing their mandates. Multilateral and plurilateral efforts to promote U.S.-and-allied-led infrastructure development can continue to be built upon. The 2022 G-7 summit featured the announcement of the Partnership for Global Infrastructure Investment. While this program has physical and digital elements, China's existing lead in Belt and Road physical infrastructure suggests that efforts to lead ahead of China could be better focused on next-generation digital technologies. Further coordination of ORAN development and deployment of ORAN technology as part of digital development programs can help to bring U.S.-and-allied technology solutions to the digital competition in the global south.

More Funding for Infrastructure & Capacity Building

If we are serious about this project, countries need to fund – at an appropriate level – infrastructure, capacity building, and cyber security programs. In terms of digital infrastructure, the U.S. CHIPS and Science Act provides for the creation of the International Technology Security and Innovation (ITSI) Fund, which provides $500 million over five years for international to provide for international ICT security and semiconductor supply chain activities, including to support the development and adoption of secure and trusted telecommunications technologies, secure semiconductor supply chains, and other emerging technologies." Combined with the U.S.-focused Department of Commerce NTIA Public Wireless Supply Chain Innovation Fund this is an opportunity to coordinate efforts to promote supply chain security, improved digital infrastructure, and projects to promote global digital development. Coordination of the NTIA efforts with those of the Department of State, as well as related activities by USAID, the U.S. Development Finance Corporation, Ex-Im Bank, National Endowment for Democracy, and others, can create a combined domestic and international

[41] U.S. Department of State, "Declaration for the Future of the Internet." Accessed March 24, 2023. https://www.state.gov/declaration-for-the-future-of-the-internet

[42] Rose Jackson, Leah Fiddler, and Jacqueline Malaret, "An introduction to the Freedom Online Coalition." *The Atlantic Council.* December 6, 2022. https://www.atlanticcouncil.org/in-depth-research-reports/report/introduction-freedom-online-coalition/

[43] U.S. Department of State, "Summit for Democracy 2023." Accessed March 24, 2023. https://www.state.gov/summit-for-democracy-2023/

approach to ICT security and infrastructure investment that better reflects the reality of friend-shored supply chains and promotes next-generation technology in development programs. The establishment of a Digital/Cyber coordinator at the U.S. Department of State enhances interagency coordination and simplifies foreign government engagement with the United States.

The lack of progress within the U.S. Congress to produce a nationwide privacy law and the inability of elected representatives to agree (so far) on competition and content moderation rules for the digital economy is without a doubt a handicap on the ability of the United States to forge digital alliances with likeminded and undecided countries. Nevertheless, this state of affairs must not deter the U.S. administration from advancing the digital freedom agenda and funding and implementing related programs.

Finally, the United States and allies can work on efforts to accelerate digital literacy and cyber hygiene education efforts, particularly for young people. While user education is not a panacea and there are differences between curriculum and issues in the countries, sharing best practices is critical. While governments should certainly encourage such dialogues and the development of digital citizenship curriculum, it is important that civil society and citizens lead the way in tackling these issues.

Conclusion & Recommendations

The authoritarian model for the internet presents a clear challenge to many cherished concepts of digital freedom that we take for granted. While there are challenges to finding consensus in many areas due to partisanship, there is agreement on the importance of securing the infrastructure that underpins our digital society. Here it is important to build secure supply chains with allies and partners, while also emphasizing continued leadership in the next-generation technologies that will underpin the future of our digital societies.

Furthermore, while we many not agree on exactly how to manage our own companies use of our data, policymakers increasingly agree about protecting our data from hostile governments. What is important in these efforts is that the process demonstrate the respect for due process, the rule of law, and civil liberties as we also protect our citizens from services and foreign actors that seek to manipulate them. Setting forward transparent but strict review processes of potentially hostile actors' access to U.S. and allied data can protect our citizens, while also ensuring that we avoid unintended consequences that harm digital commerce at home and with allies and partners. While the current attention is on TikTok, there will be other services and platforms in the future that will raise similar concerns. Additionally, given these platforms' popularity among a wide user base, any efforts by policymakers to address these security concerns should be done with bipartisan, Executive-Legislative coordination so that it does not become politicized.

Given how politicized many of the other items on the digital freedom agenda have become, international cooperation among like-minded governments—as we discuss—can help promote the digital freedom agenda with the tools that governments have available to them. However, in our model for digital society, civil society, private sector leaders, and the users themselves have as much a role, if not greater than governments, in addressing the challenges to digital freedom.

Part of this can come from a greater emphasis on digital education, though the impact there takes time, over generations. The private sector, however, can also do more in terms of transparency and the adoption of other best practices to help users avoid disinformation, enjoy safe online experiences, and trust that their data is being used in ways that they understand and consent to.

Ultimately, we must remind ourselves that the technology reflects our society. How we use it reflects our values, interests, and the careful balance of security and freedom, transparency, and privacy. How we trust our technology, our fellow citizens, and ourselves will be what ensures the future of digital freedom.

Create a holistic and strategic approach to digital freedom

This report has sought to illustrate how domestic policies and foreign collaboration on digital infrastructure security, data management, privacy protections, and content moderation combine into a holistic approach to digital freedom. Legislation and policy making should reflect the interrelated factors, and Executive and Congressional leadership should continue to promote coordination among various entities, agencies, and committees responsible.

Address U.S. policy shortcomings; promote a global vision

The United States has much to do to get its own digital house in order and promote a model that reflects U.S. and allied values. That said, as we prepare for this competition at home, getting our own policies organized will not be a silver bullet solution for global engagement. Therefore, the United States, working with allies, needs to promote simultaneously a positive digital freedom agenda on the global stage.

Promote transparency and user awareness

Digital freedom and healthy digital society requires both greater transparency in how the digital economy operates and improved user education about how their internet experience works based on the platforms they access, the algorithms delivering content, the rules for content moderation, and how to determine the veracity of what they see. While user education takes time and reflects generational shifts in awareness of and attitudes towards technology, both industry-led efforts and regulations can promote greater transparency via easily understood explanations of how sites and platforms use users' data, deliver and moderate content, and protect users' privacy.

Consider consequences and second- and third-order effects

Some proposed measures have the potential to greatly reshape the digital world. From reforms to Section 230 to data localization requirements, from federal- and state-level privacy legislation to standards set in international bodies, these proposals should be examined given their potential to create greater litigiousness, slow the internet, raise costs for consumers and individuals, and further disrupt global commerce. Legislated content moderation proposals often come into conflict with constitutional protections for speech, while also raising questions about who will be granted such censorious authorities.

Provide necessary resources and flexibility to respond to challenges to digital freedom

In terms of physical infrastructure continuing to support domestic and international "rip and replace programs" can improve infrastructure security—but only if fully resourced and with adequate hardware to replace the suspect systems. Furthermore given the importance of moving quickly to build new and next generation digital infrastructure at home and abroad, programs to upgrade digital infrastructure or to build pilot programs to deploy next generation technologies should have increased flexibility to operate both in the domestic United States as well as development programs overseas. Congress can ensure that these programs are fully resourced, while working with the Executive Branch to better coordinate the breadth of efforts in various agencies as well as their domestic and foreign remits.

Work multilaterally and with local partners on digital development

In a U.S.-China tech competition most of the world wishes to avoid being forced into a binary choice. Working with allies and partners can create multilateral approaches that share the burden while also presenting digital solutions to local partners that do not appear to be solely U.S.-driven. Furthermore in working with local partners it will be important to not only emphasize the benefits of digital freedom and continued collaboration with the United States, allies, and partners, but also to create models that allow all to benefit from the data, digital infrastructure, and value that it creates. Exploitative digital models will only fuel further suspicion and fragmentation. Using international forums like the G-7, OECD, etc. to engage with like minded partners and using the UN, the G-20, etc. to promote our vision amidst this global competition, will best leverage international forums, though opportunities for ad hoc coalitions that can move rapidly should also be embraced.

Build lasting digital partnerships

While it is true no matter the field, it also is the case in developing digital partnerships—the United States too often appears to be engaging (or re-engaging) in response to Beijing's activities or engagement. These digital freedom cooperation activities—be they supporting digital civil society, installing secure digital systems, or capacity-building in partner governments—all require consistent engagement from the United States and allies.

Acknowledgements

On behalf of the Center for the Study of the Presidency & Congress, I want to thank the following for their contributions to CSPC's work on Geotech and digital freedom: PwC Consulting, LLC, NTT, and the Dr. Scholl Foundation for their continued engagement and generosity in supporting this work.

I want to also thank all those who have engaged in these dialogues on digital freedom and worked with CSPC staff on these important policy challenges in identifying meaningful solutions. I extend my thanks to the team at the PwC Consulting's Tokyo office, and Tomoko Makino from the Foundation for MultiMedia Communications (FMMC) for their invaluable perspectives and contributions. We are also grateful to Koji Ouchi and others at the Japanese Embassy for their partnership. In addition to Japan, we are grateful to all US partners and allies who prioritize the importance of digital freedom in a global age.

I would also like to thank Priya Vora, managing director of Direct Impact Alliance, and Steven Feldstein, Senior Fellow at the Carnegie Endowment for International Peace for sharing their knowledge and expertise on Geotech and digital freedom. Lastly, I would like to acknowledge the U.S. and Japanese corporate leaders who worked with us for their vital insights into the commercial and technological aspects of this competition.

The Trustees and Counselors of CSPC, thanks to their support and wisdom, CSPC is able to ensure its mission of learning the lessons of history, address today's strategic challenges, and educating the leaders of tomorrow. Our David M. Abshire Chairholder, former House Intelligence Chairman Mike Rogers, as he continues to demonstrate his strategic vision, leadership, and a commitment to protecting the United States while championing a bi-partisan approach to national security.

Dan Mahaffee, Senior Vice President and Director of Policy at CSPC, for his leadership of this project and related corporate and transpacific outreach, as well as writing and editing many of our Geotech materials and facilitating discussion at our roundtables on digital freedom; Joshua Huminski, the Director of the Mike Rogers Center, for his research work on great power competition and technology, outreach to authors and leading thinkers, and coordination of transatlantic outreach; and CSPC Vice President Erica Ngoenha, for leading outreach to Capitol Hill and managing extensive in-person meetings, roundtables, and dialogues.

Our Senior Fellows and Advisors who contributed to this project— Hidetoshi Azuma, Ethan Brown, Samantha Clark, Rob Gerber, Andy Keiser, James Kitfield, Dr. Joshua

Walker, Zaid Zaid—who applied their expertise from a range of fields to analyze the impact of these technologies and the challenges they pose for policymakers.

Our staff and interns Kyle Flagg, Sophie Williams, Zachary Moyer Gracie Jaime for their contributions and support.

Finally, I would like to thank all of those who dedicated time to our effort by organizing and attending roundtables and offering frank and invaluable advice.

Glenn Nye
President & CEO, Center for the Study of the Presidency & Congress