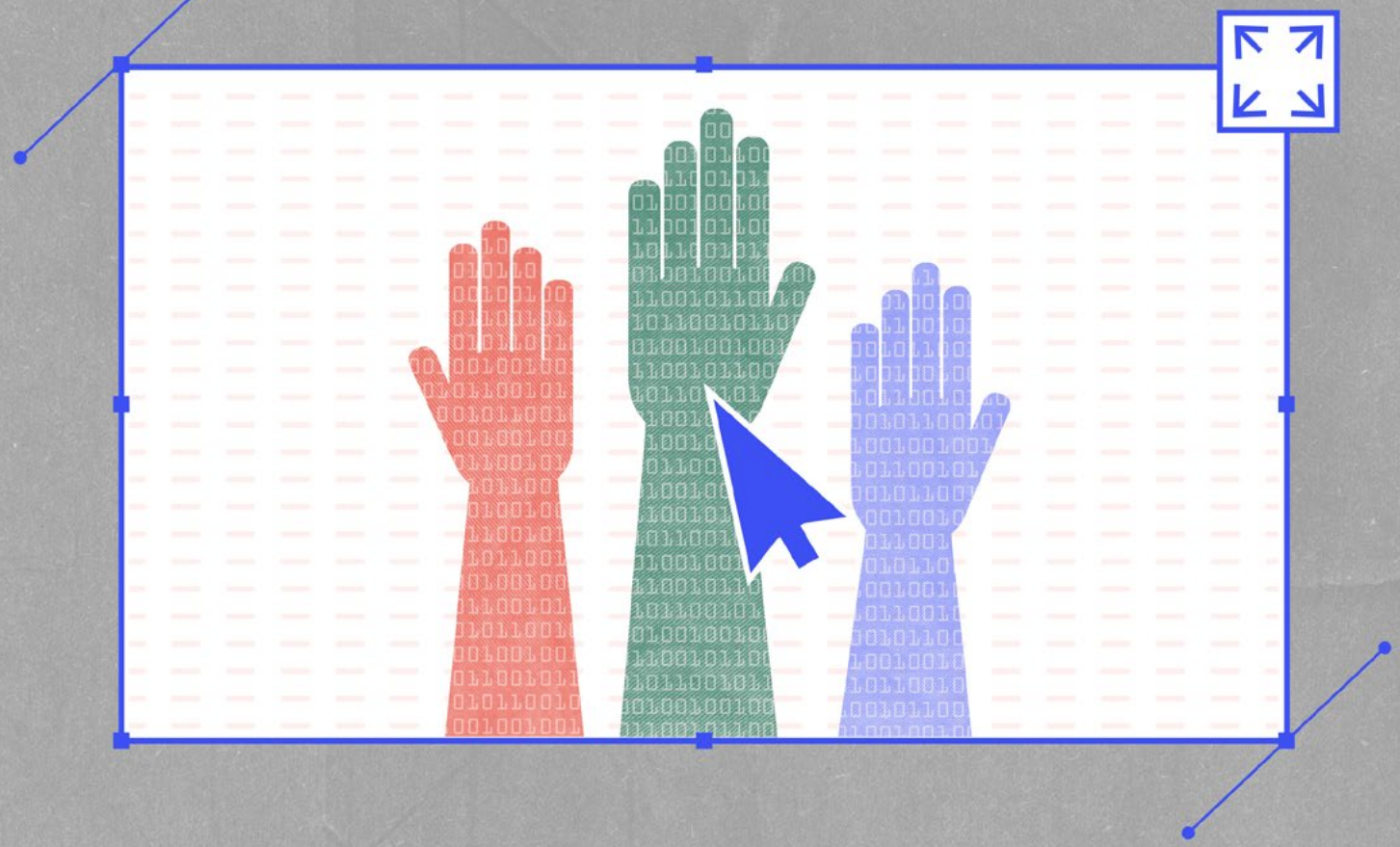
CNAS

DECEMBER 2020



Democracy by Design

An Affirmative Response to the Illiberal Use of Technology for 2021

Kara Frederick

America Competes

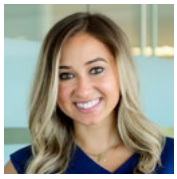
Acknowledgments

The author thanks Sheena Greitens (University of Texas at Austin), Nicole Wong (Albright Stonebridge Group), Laura Rosenberger (Alliance for Securing Democracy), Andrew Imbrie (Center for Security and Emerging Technology at Georgetown University), Shanthi Khalil (National Endowment for Democracy), Aynne Kokas (University of Virginia), the State Department, Facebook, and Google for their thoughtful feedback and suggestions.

A special thanks to the members of the Center for a New American Security (CNAS) Digital Freedom Forum, whose insights helped shape the scope and breadth of our analysis. The Digital Freedom Forum is a bipartisan effort that brings together a diverse set of stakeholders to determine how the United States should respond to the illiberal use of technology abroad, while advancing the values of freedom and openness in the digital domain. The views expressed in this report are those of the author alone and do not represent those of the forum or its members.

Thank you to Maura McCarthy, Paul Scharre, Elsa Kania, Martijn Rasser, Ainikki Riikonen, and Megan Lamberth for their reviews and clarifying conversations on all stages of the draft. Maura McCarthy, Emma Swislow, and Melody Cook provided excellent assistance in editing and graphic design. Finally, CNAS would like to thank the Quadrivium Foundation for its generous support of this and other digital freedom initiatives.

About the Author



Kara Frederick is a Fellow for the Technology & National Security Program at the Center for a New American Security (CNAS). Her research focuses on high-tech illiberalism, foreign influence operations, and digital surveillance.

Kara's analysis and commentary have appeared in *The Wall Street Journal, The New York Times, The Washington Post, Foreign Policy,* and *The Economist*. She has testified before the Senate Judiciary Subcommittee on Crime and Terrorism and is a lecturer on technology and international affairs at the George Washington University's Elliott School of International Affairs in Washington, D.C.

Prior to joining CNAS, Kara helped create and lead Facebook's Global Security Counterterrorism Analysis Program. She was also the team lead for Facebook Headquarters' Regional Intelligence Team in Menlo Park, California. Prior to Facebook, she served as a Senior Intelligence Analyst for a U.S. Naval Special Warfare Command and spent six years as a counterterrorism analyst at the Department of Defense. While at the Department of Defense, she deployed three times to Afghanistan in support of special operations forces, served as a briefer to the Assistant Secretary of Defense for Special Operations/Low Intensity Conflict, and served as a liaison to the National Security Agency.

She received her MA in war studies from King's College London and her BA in foreign affairs and history from the University of Virginia.

America Competes

2020

America Competes 2020

America Competes 2020 is a Center-wide initiative featuring cutting-edge CNAS research, publications, events, and multimedia aimed at strengthening the United States' strategic advantages at home and abroad.

TABLE OF CONTENTS

Chinese telecommunications firm Huawei's attempts to build much of the world's next generation wireless networks galvanized democracies to push back, citing national security concerns. Here, the company displays a facial recognition camera on the Huawei campus in Shenzhen, China, in 2019. (Kevin Frayer/Getty Images)

Executive Summary

A global contest between democracies and autocracies is raging on the digital front. Technology stands to alter the balance between free, open societies and closed, repressive regimes. Nation states in direct competition with the United States seek to project global influence by shaping an existing digital order to their will. Impulses toward illiberal use of technology at home threaten to curtail individual liberties, constrict opportunity, and erode a truly open society.

Democracies do not yet have a model for how to confront this. In the United States, a roadmap for a solution must start with the fundamental question: How should U.S. technology companies, with the help of the U.S. government, respond to the illiberal use of technology by authoritarian actors abroad? This report contends with this question by identifying concrete actions and threat-mitigating strategies that contain the input of government, the tech sector, civil society, and academia. It provides starting points to address the systemic risk inherent in dealing with authoritarian regimes and also examines cost imposition on those complicit in tech-enabled human rights abuses.

Yet a strategy aimed only at staunching the illiberal use of technology will fail in the long term. Instead, the U.S. government and tech companies alike must recruit democratic allies to purvey an affirmative agenda that promotes digital freedom across the globe. This report proposes an agenda that stresses privacy leadership by the United States and its technology companies. It identifies areas of collaboration for U.S. allies and democratic partners, like digital trade, foreign law enforcement requests for data, and technical standards. This report's affirmative agenda also contains an imperative for U.S. tech companies to build commercial norms toward digital freedom and incentivize transparency within their own ranks.

For digital freedom to prevail over authoritarian uses of technology, democracies must present something better. Together, they must establish an alternative model for the use of technology globally. These recommendations build that democratic case, starting with the United States.

Summary of Recommendations

Address Systemic Risk through Existing Federal Mechanisms

To help U.S. private companies address systemic risk when operating abroad, the U.S. State Department (DoS) should:

- Integrate a host country's digital practices into its annual Country Reports on Human Rights Practices, also known as Human Rights Reports.
- Work with the Commerce Department to update its Country Commercial Guides to incorporate a set of key indicators of authoritarian digital practices abroad.
- Update the Country Commercial Guides to include these new indicators, as well as feedback from willing partners in civil society and the tech industry, on an annual basis.
- Hold formal consultations with U.S. tech companies every two years on the utility of providing information on the risks associated with aiding authoritarian governments.
- Regularly update its risk-based compliance framework for surveillance technology due diligence, in coordination with the Department of Commerce and other relevant agencies.
- Take steps to make human rights end use due diligence compliance legally binding, instead of voluntary. This includes coordinating with the Department of Commerce's Bureau of Industry and Security (BIS) to expand export controls based on end use.[1]

To address systemic risk, U.S. universities should consider the following courses of action:

- Rethink engagement with authoritarian countries writ large, based on indicators of systemic risk arising from involvement with these countries and the shift to online learning due to the COVID-19 pandemic.[2]
- Comply with U.S. government human rights guidance based on end use from the State Department and entity listings from the Department of Commerce.
- Conduct own due diligence on individuals, organizations, and end uses of academic research by instituting an internal human rights research review board.
- Integrate human rights standards and training into business and engineering curricula.
- Develop guidelines for assessing national security risk in funding sources and research collaborations.

Impose Costs on Tech-Enabled Human Rights Abuses

To impose costs on actors committing tech-enabled human rights abuses, the U.S. government (legislative, executive, and federal agencies as specified) should:

- Audit the current decision-making process used to inform federal actions aimed at confronting high-tech illiberalism. Specifically, the White House should bring together multiple agencies, starting with the DoS, Commerce, and Treasury, to survey the existing federal toolkit—sanctions, bans, suspensions, and divestment—and consider alternative measures to slow or prevent investment in technologies and tech actors that enable human rights abuses.
- Harmonize these multi-pronged approaches, adjudicate decisions, and take into account all stakeholders in the process via the National Security Council (NSC), in coordination with the National Economic Council (NEC) and the Office of Science and Technology Policy (OSTP).[3]

Establish an Affirmative Agenda for Digital Freedom

This affirmative agenda consists of three main concepts: lead in privacy, find areas of mutual cooperation with democratic partners and allies (e.g., digital trade, foreign law enforcement requests for data, and technical standards), and enlist and support tech companies' construction of commercial norms toward digital freedom.

LEAD IN PRIVACY

Congress should:

- Establish a federal data protection framework with appropriate standards and oversight for how the federal government and commercial entities collect, store, and share U.S. user data.[4]
- Articulate and publish a public justification for this framework that describes the fundamental elements of a strong privacy regime.
- Mandate that the Federal Trade Commission (FTC) enforces privacy legislation.

Congress and the White House should also:

- Fund the research and development of privacy-preserving technology solutions through the National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), a restored Open

A fixture on Capitol Hill in Washington, D.C., U.S. tech CEOs will be critical in implementing any federal data protection framework. On November 17, 2020, Facebook CEO Mark Zuckerberg testified before the Senate Judiciary Committee in a hearing titled "Breaking the News: Censorship, Suppression, and the 2020 Election." (Bill Clark/Pool/Getty Images)

Technology Fund (OTF), and the DoS, particularly the Bureau of Democracy, Human Rights, and Labor (DRL).

- The U.S. government also should fund the research and development of privacy-preserving and democratic models of surveillance authorities, utilizing bilateral solutions, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act, to better coordinate with partners.

U.S. tech companies should:

- Devote engineering capacity to designing protocols with built-in data privacy protections.
- Invest in "interoperable privacy" to ensure the feasibility and endurance of this privacy regime with those of democratic allies.
- Similarly, invest in privacy compliance, as well as privacy preservation, to solidify strong privacy practices hand-in-hand with the federal government.

FOCUS ON AREAS OF MUTUAL COOPERATION WITH ALLIES AND PARTNERS: DIGITAL TRADE, FOREIGN LAW ENFORCEMENT REQUESTS, AND TECHNICAL STANDARDS[5]

To keep digital trade open, the Office of the United States Trade Representative (USTR) should:

- Strengthen digital trade language in free trade agreements to enable the free flow of data and regulatory interoperability between allies through the global expansion of the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System.

To help ensure foreign-generated law enforcement data requests and compliance are consistent with democratic values and to strengthen collaboration with like-minded partners globally, the DoS and Department of Justice (DOJ) should:

- Leverage the CLOUD Act to seek bilateral and even multilateral agreements on foreign law enforcement data requests to U.S. companies with governments that honor baseline principles of digital freedom, open digital trade, privacy, human rights, and due process.

To promote digital freedom through international standards organizations with like-minded partners, the Secretary of Commerce should:

- Issue a plan for federal engagement in developing technical standards for surveillance technologies, akin to the 2019 NIST plan to advance artificial intelligence (AI) standards and research priorities.

To promote digital freedom through international standards organizations with like-minded partners, Congress and the White House should:

- Expand federal support of standards developing organizations (SDOs) to ensure that outcomes (standards and regulatory recommendations) related to technologies prone to abuse by authoritarians, such as AI-related tech, are more supportive of digital freedom.[6]

To promote digital freedom through international standards organizations with like-minded partners, U.S. universities should:

- Leverage U.S. involvement in the development of International Organization of Standardization/ International Electrotechnical Commission (ISO/IEC) standards, such as 24368 'AI overview of ethical and societal concerns' and 24027 'Bias in AI systems and AI aided decision making.'[7] Duly, implement training on the ethical and responsible use and development of technology in science, technology, engineering, and mathematics (STEM) curricula, with an emphasis on algorithm design. This inclusion of the appropriate considerations surrounding AI ethics and bias in curriculum design will allow for the enhancement of STEM curricula in alignment with international standards.

Belied by its exterior, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) building houses forward-leaning technical efforts to develop the standards that will determine the rules of the road for the global use of technology. (Dana Romanoff/Getty Images)

ENLIST TECH COMPANIES TO BUILD COMMERCIAL NORMS TOWARD DIGITAL FREEDOM

To build norms that promote digital freedom and incentivize transparency, U.S. tech companies should:

- Develop guidance for responsible release of novel emerging technologies that are susceptible to abuse (e.g., leverage examples such as Open AI's staged release of GPT-2 language model) to build norms around responsible release.
- Continue to advance efforts to safeguard user security and privacy, including through technology such as encryption and other privacy-preserving technologies.
- Consider publicizing voluntary, biannual public reports on policies and intent regarding data collection, storage, and sharing.

Introduction

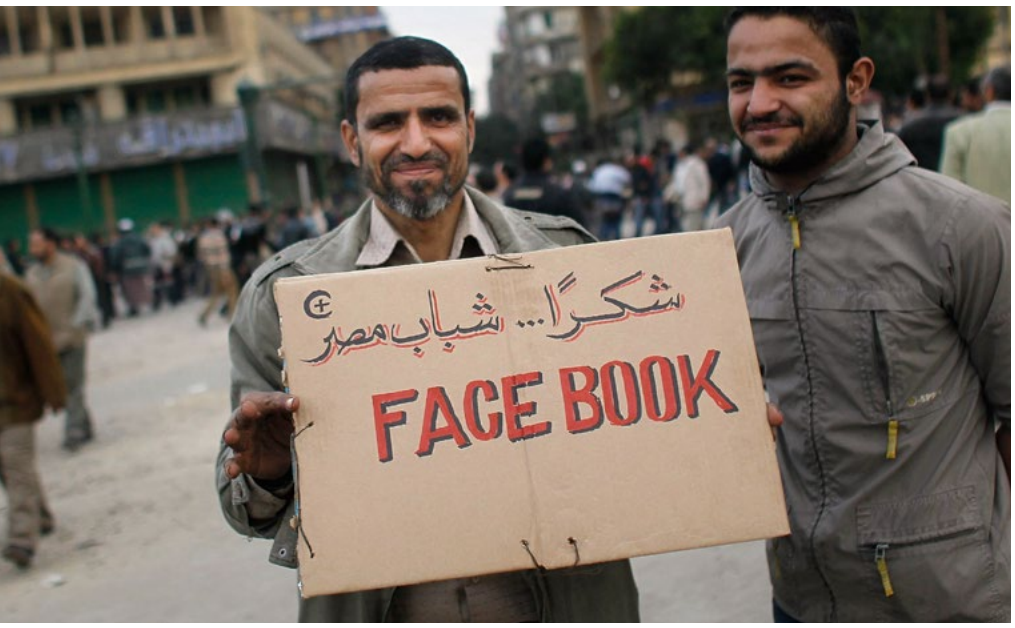
Technology was supposed to be the great "democratizer" of our age. The advent of the internet and social media promised to wrest control of information from the hands of a few and distribute it to many. It promised to materially improve quality of life while airing marginalized perspectives, elevating new views in a meritocracy of ideas, and even propagating a more open society.

Reality besieged that vision. Authoritarians have taken advantage of these tools to bolster internal stability, supplement their data reserves, enrich their coffers, and rise in global influence. Many countries continue to draw inspiration from China's example of digital surveillance and internal control, which combines "cyber sovereignty" with ambiguous, widely-scoped laws to boost state control. Compounding this are challenges for tech companies and U.S. consumers alike, such as evolving data localization laws and host nation demands for data from private U.S. companies. Other challenges of high-tech illiberalism include: the expansion and export of data-guzzling platforms subject to authoritarian governments, the proliferation of intrusive surveillance technology, tech-enabled human rights abuses, information control, and ineffective data security and privacy measures on global digital platforms.

The illiberal use of certain technologies and platforms tears at the fabric of open societies too. U.S. entities, including industry and universities, have contributed to digital repression abroad by exporting equipment, software, expertise, and training data.[8] At home, surveillance capitalism and "ad-tech" imperil user privacy. Unaccountable algorithms and unsecured facial recognition databases threaten individual liberties, even in democratic societies.

But democracies approach these problems differently. The rule of law and existing norms help, albeit imperfectly, to curtail abuse of technology by democratic governments and private companies. In contrast to authoritarian regimes, democracies openly debate the merits of different approaches. They tap a diverse set of stakeholders to adjudicate outcomes, often slowly and from the ground up.[9] The United States must leverage these features of its process to formulate a clear alternative to the authoritarian use of technology.

This report aims to build on the intrinsic advantages of the democratic process—transparency, inclusivity, and deliberation—to create a framework for how the U.S. federal government, tech companies, and universities should respond to the illiberal use of technology abroad.[10] Private sector leaders, policymakers, academics, and civil society experts are critical to the success of this effort. Likewise, the U.S. companies that develop and maintain digital platforms across the globe must also defend open societies and individual freedom. Invariably, these companies are central to the survival and future of individual liberty in the 21st century. This report designates the roles and responsibilities of these players, discusses ways to foster and enact specific principles, and recommends concrete actions to build an affirmative agenda that promotes digital freedom together with democratic partners.



From 2010 onward, dissidents relied on social media to organize protests during the Arab Spring. Technology promised to be a great "democratizer," in more ways than one. Reality turned out to be more complicated. This image depicts protestors demonstrating against then-President of Egypt Hosni Mubarak in Tahir Square in Cairo, Egypt, in 2011. (Chris Hondros/Getty Images)

Address Systemic Risk through Existing Federal Mechanisms

The current U.S. approach to digital authoritarianism often amounts to ad-hoc fixes that do not account for the holistic threat atmosphere, despite recent surges in activity from 2019 to 2020 by the White House, State Department, Treasury Department, and Commerce Department.[11] In the same vein, existing U.S. laws and regulations do not offer an enduring roadmap to help U.S. tech companies counter repressive digital practices abroad. Solutions require identifying and mitigating the systemic risk that arises from dealing with authoritarian governments.[12] Systemic risk consists of the threats that are intrinsic to systems of governance distinct from, or opposed to, free and open societies. Characteristics that distinguish authoritarian regimes from open societies and that are relevant to the digital environment include, but are not limited to: more intrusive data practices not subject to legal recourse; an illiberal legal and governance atmosphere (e.g., China's 2017 National Intelligence Law and Hong Kong's 2020 national security law); a state-led economic system; a lack of an independent judicial system; lack of the rule of law; the absence of representative, democratic governance; and lack of free, independent media institutions.

These systemic risks are independent from specific companies or technology use cases within these societies. Rather, these risks are intrinsic to the system of governance and arise from dealing with actors beholden to or exporting what the European Commission refers to as "alternative models of governance," rendering them in "systemic" competition with democratic actors.[13] Even if a particular company is not (at present) engaged in abusive practices, a company operating within a nation subject to this form of governance is at risk of the government's coercive power. Moreover, a company could find themselves without recourse to an independent judiciary to sue the government or a free press to shine a light on government abuses. The U.S. government must assess and identify indicators that capture these threats to help inform the due diligence practices and risk assessments of U.S. tech companies for the digital environment.

> **Solutions require identifying and mitigating the systemic risk that arises from dealing with authoritarian governments.**

The Hong Kong government's deepening relationship with the Chinese Communist Party and increasing authoritarianism, demonstrated by the approval of a restrictive national security law in 2020, is cementing an atmosphere of illiberal governance. Here, a protestor is arrested at an anti-government demonstration in September 2020 in Hong Kong. (Anthony Kwan/Getty Images)

The absence of a framework to assess this risk is particularly detrimental for U.S. tech companies. Tech companies are on the frontlines of this battleground, often improvising and testing policies and practices as they operate in undemocratic nations. A U.S. government-built framework to assess systemic risk would enable commercial entities to maintain their global footprint and responsibilities to users outside of the United States. Top-down guidance and resources would help flag and avoid complicity in authoritarian abuses. This framework would also help provide an official rationale for private companies to decline malign actors' requests for cooperation abroad. In turn, tech companies can identify lessons learned from operating abroad and inform the U.S. government of their best practices to help them address the next challenge together.

Finally, the U.S. government can aid U.S. universities in responding to potential digital repression by malign, foreign actors. These institutions face challenges similar to tech companies in managing research and funding partnerships with national security implications. They are also dealing with a new digital battlefront due to an overwhelming shift to virtual learning during the COVID-19 pandemic, their ability to proliferate norms through education, and the prodigious international talent and intellectual property considerations within their walls. A risk-based framework for handling these challenges would provide academia with a robust vehicle for identifying and assessing digital threats emanating from authoritarian regimes.

To help U.S. private companies address systemic risk, the State Department (DoS) should:

- **Integrate a host country's digital practices into its annual Country Reports on Human Rights Practices, also known as Human Rights Reports.** The guides should define what "abuse" of technology constitutes to help companies create their own rulesets to respond to the illiberal use of their technology abroad. Key indicators for abuse include, but are not limited to:
  - » Aggregation of institutional data with established intent of political or social control (e.g., development of a "national architecture" for data collection);
  - » Track record of exporting to and investing in surveillance systems for regimes with poor human rights records;
  - » Low ranking on combined digital rights indexes (e.g., how well countries perform regarding digital privacy);
  - » Systemic risk due to the state's political institutions or nature of their legal order and legal frameworks (e.g., low strength of civil society oversight and the lack of an independent judiciary, free press, rule of law, and mechanisms for recourse against government demands for data).
- **Work with the Commerce Department to update its Country Commercial Guides to incorporate a set of key indicators of authoritarian digital practices abroad.** The aim is to help U.S. tech companies assess levels of risk associated with a host government's potential abuse of user data, especially U.S. consumer data, (e.g., excessive surveillance, indefinite storage, etc.) when operating abroad.
- **The Country Commercial Guides should continue to be updated annually with the inclusion of these new indicators, as well as feedback from willing partners in civil society and the tech industry.** The DoS should solicit input from research organizations like Freedom House and Ranking Digital Rights, as well as other civil society actors via a mediated process for continued feedback on these specific indicators.[14]
- **Hold formal consultations with U.S. tech companies every two years on the utility of providing information on the risks associated with aiding authoritarian governments.**
  - » These consultations could further serve to solicit ideas from tech companies on what information or what new indicators would help refine and orient their operating practices toward digital freedom.
  - » In return, tech companies can communicate what they are doing right and share their best practices with the DoS to help them anticipate the next challenges together. This would also help the DoS update their Country Commercial Guides and issue-based due diligence reports with any new risk indicators directly from the practitioners themselves.
- **Regularly update its risk-based compliance framework for surveillance technology due diligence in coordination with the Department of Commerce and other relevant agencies.** The State Department's Bureau of Democracy, Human Rights, and Labor (DRL) should update levels of risk based on updates to foreign statutes related to data collection (e.g., China's 2020 Foreign Investment Law) and tech advancement regarding systems with high risks of contributing to repression (e.g., export controls on "crime-control products" destined for use by the Chinese Communist Party).
- **Take steps to make human rights end use due diligence compliance legally binding, instead of voluntary.** This includes coordinating with and expanding export controls based on end use by the Department of Commerce's Bureau of Industry and Security (BIS).[15]

To address systemic risk, U.S. universities should consider the following courses of action:

- **Rethink engagement with authoritarian countries writ large, based on indicators of systemic risk arising from engagement with these countries and the shift to online learning due to the COVID-19 pandemic.**[16]
- **Comply with U.S. government human rights guidance based on end use from the State Department and entity listings from the Department of Commerce.** Other reasonable aspects of this calibrated approach to engagement with authoritarian actors include:[17]
  - » A ban on partnering with individuals or organizations on the BIS Entity List.
  - » Compliance with DoS voluntary guidance on human rights due diligence and use of BIS's "Know Your Customer Guidance" and red flag indicators to assess potential partnerships.[18]

- **Conduct own due diligence on individuals, organizations, and end uses of academic research by instituting an internal human rights research review board.** This review board would address potential research collaborations with institutions or individuals from countries committing human rights abuses. Its remit would include due diligence on individuals, organizations, and end uses of academic research.[19]
- **Integrate human rights standards and training into business and engineering curricula.**
- **Develop guidelines for assessing national security risk in funding sources and research collaborations.**
  - » Liaise with and leverage the FBI, the U.S. Intelligence Community, and the DoS at appropriate levels of classification to establish baseline knowledge of and identify the indicators of systemic risk (the varying set of risks inherent to undemocratic societies and closed systems) associated with specific industry and academic partnerships.
  - » Implement restrictions on lab access if individuals meet the risk threshold specified by these federal interlocutors.
  - » Reinvigorate existing mechanisms to enable exchange and feedback loops between academia and the government, especially when establishing data security practices.

Impose Costs on Tech-Enabled Human Rights Abuses

Authoritarian regimes use cutting-edge technologies to control and oppress their citizens at home and undermine democracies and open societies abroad. Democracies, with the United States in the lead, can resist this through a series of measures.[20] The United States has an existing toolkit for imposing costs on actors—both at home and abroad—that propagate digital repression. Measures include the Commerce Department's actor-based entity listings, which effectively block U.S. companies from exporting to entities tied to activities contrary to U.S. national security or foreign policy interests.[21] Other related, legally binding tools include Commerce's export controls, which regulate the release of certain technologies, and Treasury sanctions via the Office of Foreign Assets Control (OFAC).

The need for a comprehensive regulatory regime that combines additional sanctions authorities with the expansion of export controls based on end use is essential.[22] As CNAS scholars proposed in December 2019:

> "...the U.S. Commerce Department should undertake the development of a new export control regulation that would restrict the sale of both key U.S.-origin products and key foreign-origin products developed by U.S. companies and their subsidiaries overseas to be used for certain end uses in China, including those that infringe on internationally accepted human rights standards, enable surveillance or cyberespionage, and are involved in domestic security activities."[23]

The United States requires a multi-pronged approach that consists of both actor-based regulations and expanded end-use based export controls to confront high-tech illiberalism, particularly by China.[24] In addition, the federal government should continue to strongly consider the use of additional tools, such as the International Emergency Economic Powers Act (IEEPA) or Committee on Foreign Investment in the United States (CFIUS) investigations.

But it can go one step further. To maximize the impact of these tools, the U.S. government should establish a coherent process to bring them together, including: actor-based regulations, end-use based export controls, and the separate assortment of policy levers like IEEPA and CFIUS. The U.S. government must restructure its interagency processes to adjudicate these decisions and

take into account a diverse set of stakeholders.[25] Federal government processes to confront this multi-faceted set of risks must be coordinated and organized across agencies in a more deliberate manner.

The United States should pursue an expanded export control regime in full recognition of potential second- and third-order effects. These effects could include incentivizing less values-conscious foreign competitors to take advantage of gaps in the market. Restricting U.S. actors from contributing to human rights abuses may spur indigenous innovation and development of technology by or under authoritarian governments in its place. While the goal should be to prevent U.S. actors from committing human rights violations, indigenous innovation would also be problematic for open societies in a number of ways. First, a poor track record of such technologies on user privacy protections, security vulnerabilities, intrusive data practices, and data governance measures would imperil user privacy and security.[26] Further, based on the rapid diffusion of Chinese-built surveillance systems to undemocratic regimes, this indigenous development could result in global proliferation, creating a more fractured and closed digital landscape.[27]

The United States requires a multi-pronged approach that consists of both actor-based regulations and expanded end-use based export controls to confront high-tech illiberalism, particularly by China.

The United States should look to its competitive advantage: a free and open society that has been the engine of the world's innovation for multiple generations.[28] It must play to these strengths and continue to dictate the design of products the world uses. It must create and offer attractive, commercially viable alternatives to technologies developed under and beholden to undemocratic governments. This way forward is detailed in the final section of this report.[29]

To impose costs on actors committing tech-enabled human rights abuses, the U.S. government (legislative, executive, and federal agencies as specified) should:

- **Audit the current decision-making process used to inform federal actions aimed at confronting high-tech illiberalism.** Specifically, the White House should bring together multiple agencies, starting with the DoS, Commerce, and Treasury, to survey the existing federal toolkit—sanctions, bans, suspensions, and divestment—and consider alternative measures to slow or prevent investment in technologies and tech actors that enable human rights abuses.
  - » Require tech companies from states with poor human rights records to submit human rights documentation as part of the U.S. Securities and Exchange Commission registration process.
  - » Encourage commitment to the United Nations Guiding Principles on Business and Human Rights, as well as public disclosure of human rights due diligence on a recurring basis.
  - » Require foreign companies listing securities on U.S. exchanges to meet the same audit and disclosure requirements needed by U.S. firms.[30]
  - » In concert with the use of the Entity List, the executive branch should consider additional Magnitsky Act sanctions and Leahy Law restrictions if partners or potential partners are found to be complicit in tech-enabled human rights abuses.
  - » Continue to use of IEEPA suspensions (e.g., a ban on importation or distribution of Chinese-controlled social media services/apps) or divestment via the CFIUS.
- **Harmonize these multi-pronged approaches, adjudicate decisions, and take into account all stakeholders in the process via the National Security Council (NSC), in coordination with the National Economic Council (NEC) and the Office of Science and Technology Policy (OSTP).**[31]
  - » The NSC should establish an interagency working group aimed at restructuring and formalizing a coordinated, multi-agency process to arbitrate decisions related to tech-enabled infringements on U.S. values and interests. These infringements include tech-enabled human rights abuses and digital surveillance.
  - » Invite international human rights organizations to the table and continue to expose tech-enabled gross violations of human rights by nation-states and linked actors, such as the use of the Integrated Joint Operations Platform to target Uighur Muslims in Xinjiang.

Establish an Affirmative Agenda for Digital Freedom

The United States must articulate and establish a positive agenda for addressing digital authoritarianism. America needs to be *for* a specific set of principles, and not simply play defense against Russian bots and Chinese surveillance systems. This affirmative agenda should start with a strong privacy regime at home. Simultaneously, the United States should harmonize approaches to specific digital issues with like-minded allies. Issues like digital trade, foreign law enforcement requests, and tech standards can serve as initial areas of collaboration for democratic governments and digital media companies. How rights-respecting democracies collaborate and solve these problems will serve as the bedrock of an enduring technology alliance. Fostering a multilateral, democratic approach—rather than a purely American one—to these issues stands to link a bloc of countries together in pursuit of digital freedom.[32] Finally, the commercial sector must build norms that explicitly foster digital freedom—norms that advance an open internet, the free flow of data, user privacy, transparency, and resistance to illiberal uses of technology.

The commercial sector is integral to establishing norms of privacy and transparency for new technologies. Here, Twitter CEO Jack Dorsey testifies virtually in front of the Senate Judiciary Committee on November 17, 2020. (Hannah McKay/Pool/Getty)

Lead in Privacy

Privacy will be the new coin of the digital realm. As such, privacy leadership should be the linchpin in a U.S.-led affirmative agenda for digital freedom. This leadership consists of articulating and establishing a strong privacy regime for federal government and commercial use, and fostering these principles within a new federal privacy law. Privacy leadership should culminate in the establishment of a federal data protection framework and a designated enforcement authority for this legislation.

Privacy will be the new coin of the digital realm. As such, privacy leadership should be the linchpin in a U.S.-led affirmative agenda for digital freedom.

Relatedly, U.S. companies are leaders in technological solutions to data protection. Tech companies should devote resources to enshrine privacy protections and transparency directly in their design. This includes tailoring investments toward data encryption, federated models of machine learning, and differential privacy—the withholding of certain forms of personally identifiable information while still sharing other, less personal data. These models consist of machine learning approaches that avoid transferring data from individual devices to a central data repository, making personal data less likely to be exploited by actors with access to that repository. Such approaches would thwart some authoritarians' ambitions of synching multiple data sources together, such as with China's social credit system, to more effectively automate control. Additional research can establish global examples for privacy solutions that advance democratic values by protecting dissidents and prioritizing individual liberty. U.S. tech companies should not only focus on developing these privacy-preserving technologies, but also invest in privacy compliance to help cultivate robust privacy practices that work *with* and not *against* U.S. authorities.

For the federal government to lead in privacy, Congress should:

- **Establish a federal data protection framework with appropriate standards and oversight for how the federal government and commercial entities collect, store, and share U.S. user data.**[33] The initial focus of the effort should:
  - » Establish clear policies on data retention, such as time limits and the prohibition of infinite data storage.
  - » Categorize biometric data as "sensitive data" with additional protections based on risk assessments, including limited interoperability. Require consent before collecting and processing this data.
  - » In a federal privacy law, set collection and use limitations on sensitive information based on evaluation of that type of data, especially for facial recognition technology. Ensure that acquisition of such sensitive data is strictly controlled by the designated enforcement authority.
  - » Ensure U.S. government identity management systems are secure, reliable, and based on National Institute of Standards and Technology (NIST) guidelines. Congress should mandate data protection inspections and oversight.
  - » Ensure a consistent national standard by preempting state laws to avoid an increasing patchwork of inconsistent state obligations.
- **Articulate and publish the fundamental elements of a strong privacy regime, including:**
  - » American citizens and consumers should have basic rights over their information that they can expect to be honored by any entity that holds it, as well as meaningful recourse in the event their rights are not honored.
  - » Organizations that hold American citizens' and consumers' data should be subject to basic obligations to handle that data responsibly, including by robust oversight of their data-sharing relationships with third parties.
- **Mandate that the Federal Trade Commission (FTC) enforces privacy legislation.** A dynamic and forward-thinking regulator that embraces innovative regulatory models to support evidence-based policymaking and is empowered to provide recourse for customer complaints should enforce these obligations.

Privacy issues are not distinct to authoritarian regimes. In the wake of the 2015 San Bernardino terrorist attacks, Apple resisted a series of requests by the FBI to create a "backdoor" to the iPhone that would allow federal law enforcement access to one of the attackers' devices. In 2016, a handful of protestors, pictured, gathered in front of FBI headquarters in Washington, D.C., to support Apple's appeal to the U.S. judicial branch. (Chip Somodevilla/Getty Images)

Congress and the White House should also:

- **Fund the research and development of privacy-preserving technology solutions through the NIST, the National Science Foundation (NSF), a restored Open Technology Fund (OTF), and the DoS, particularly the DRL.** Include executive branch agencies' chief privacy officers in these efforts and coordinate through the International Trade Administration (ITA) to ensure technological solutions align with the United States' international commitments on privacy—bilaterally and through multilateral organizations such as the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC).
- **The U.S. government also should fund the research and development of privacy-preserving and democratic models of surveillance authorities, utilizing**

bilateral solutions, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act, to better coordinate with partners.

For U.S. industry to lead in privacy, U.S. tech companies should:

- **Devote engineering capacity to designing protocols with built-in data privacy protections,** such as privacy by design; federated learning models; decentralized networks where access and control is distributed among multiple machines instead of housed in a central server; new navigation protocols that introduce an additional layer of privacy to confer more user control, like encrypted Domain Name System; and methods of encryption.
- **Invest in "interoperable privacy" to ensure the feasibility and endurance of this privacy regime with those of democratic allies.**
- **Invest in privacy compliance, as well as privacy preservation, to solidify strong privacy practices hand-in-hand with the federal government.** Tech companies should engage Commerce, the DoS, and the FTC to further amplify compliance with existing NIST privacy compliance standards.

Focus on Areas of Mutual Cooperation with Allies and Partners: Digital Trade, Foreign Law Enforcement Requests, and Technical Standards[34]

Democracies should identify areas of collaboration and formalize exchanges over digital trade, foreign law enforcement requests, and technical standards. This focus on setting international standards would help promote digital freedom with like-minded partners globally. It could also lay the groundwork to convene a bloc of democracies, similar to Britain's "D10" approach to next generation wireless, or a new "Tech Alliance" to safeguard liberal-democratic institutions and to act as a bulwark against authoritarian powers.[35] Once convened, these countries should articulate approaches to the following areas based off of an agreed-upon set of principles that advance digital freedom.

To keep digital trade open, the Office of the United States Trade Representative (USTR) should:

- **Strengthen digital trade language in U.S. free trade agreements to ensure the free flow of data and regulatory interoperability between allies through the global expansion of the APEC Cross Border Privacy Rules (CBPR) System.** USTR should simultaneously push back on foreign digital trade restrictions (data localization, digital sovereignty, etc.) that increase state control over user data and decrease internet freedom and openness.

To ensure foreign-generated law enforcement data requests and compliance are consistent with democratic values and to strengthen collaboration with like-minded partners globally, the DoS and Department of Justice (DOJ) should:

- **Leverage the CLOUD Act to seek bilateral and even multilateral agreements on foreign law enforcement data requests to U.S. companies with governments that honor baseline principles of digital freedom, open digital trade, privacy, human rights, and due process.** This would strengthen and consolidate a bloc of allied nations around expanded information-sharing agreements primarily based on their commitment to rule of law and other democratic principles. It would stand to provide a potential basis for expanded information-sharing arrangements between the private and public sectors of different democratic nations.[36]

To promote digital freedom through international standards organizations with like-minded partners, the Secretary of Commerce should:

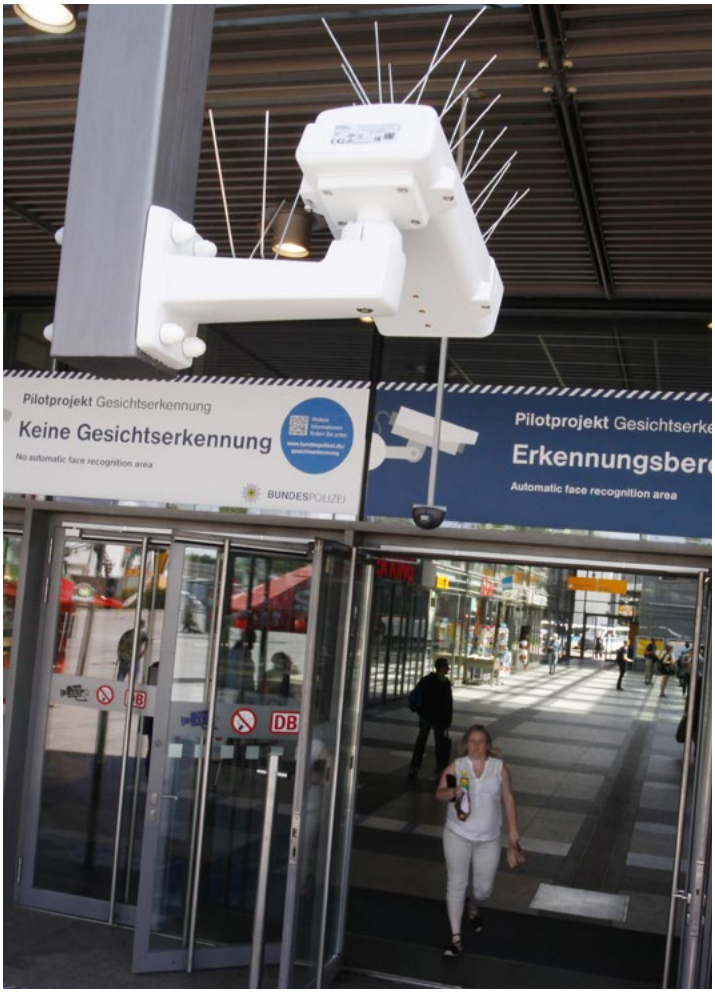
- **Issue a plan for federal engagement in developing technical standards for surveillance technologies, akin to the 2019 NIST plan to advance artificial intelligence (AI) standards and research priorities.** This plan should mirror NIST's proactive approach to AI standard-setting by suggesting minimum thresholds for appropriate submissions to international standards developing organizations (SDOs). The intent is to boost U.S. engagement in international standards bodies and other international organizations regarding technologies with potential for illiberal use, such as facial recognition systems.

To promote digital freedom through international standards organizations with like-minded partners, Congress and the White House should:

- **Expand federal support of SDOs to ensure that outcomes (standards and regulatory recommendations) related to technologies prone to abuse by authoritarians, such as AI-related tech, are more supportive of digital freedom.**[37]
- **Actively contribute to and engage with industry leaders working on standards for privacy and protection of users' digital data.** For example, the United States should refer to and provide input to the following: International Organization for Standardization (ISO)/Project Committee 317 'Consumer protection:

privacy by design for consumer goods and services,' ISO/International Electrotechnical Commission (IEC) Joint Technical Committee 1/Subcommittee 27 'Information security, cybersecurity and privacy protection,' ISO/IEC Committee draft 27556.2 'User-centric framework for the handling of personally identifiable information,' ISO/IEC 27557 'Organizational privacy risk management,' and ISO/IEC 27550 'Privacy engineering for system life cycle processes.'[38]

- **Identify opportunities to support U.S. industry engagement in additional organizations working on AI standards around data use, trustworthiness, and use in video surveillance, such as ISO/IEC subcommittee on AI (SC42) and the Institute of Electrical and Electronic Engineers series for affecting "Human Well-Being."[39]**



As surveillance and other technologies prone to abuse proliferate, the United States can work with its democratic partners to ensure digital systems err toward digital freedom. Here, German federal police test a facial recognition system outside the Suedkreuz train station in Berlin in the summer of 2017. (Michele Tantussi/Getty Images)

To promote digital freedom through international standards organizations with like-minded partners, U.S. universities should:

- **Implement training on the ethical and responsible use and development of technology in science, technology, engineering, and mathematics (STEM) curricula, with an emphasis on algorithm design.** Leverage U.S. involvement in the development of ISO/IEC standards, such as 24368 'AI overview of ethical and societal concerns' and 24027 'Bias in AI systems and AI aided decision making,' to include the appropriate considerations surrounding AI ethics and bias in curriculum design.[40] This will allow for the enhancement of STEM curricula and alignment with international standards. Consider tying these training imperatives to public funding or certifications.

Enlist Tech Companies to Build Commercial Norms toward Digital Freedom

Norm building is no longer the province of nation states alone. Commercial actors already work together to develop and employ charters and agreements on specific norms in cybersecurity, AI, and other fields.[41] Companies should use such agreements as blueprints to create their own norms surrounding digital freedom. Tech companies can articulate company-wide principles that protect and advance digital freedom and recruit other corporate actors to support this declaration of norms.

Further, U.S. tech companies are the new prime movers in the fight against digital repression. They should run their businesses in a way that fosters an open internet and free flow of data. They should steadfastly push back against data localization laws or other domestic data and privacy related laws that fail to conform to human rights standards. Part of this initiative

Norm building is no longer the province of nation states alone. Companies should use such agreements as blueprints to create their own norms surrounding digital freedom.

includes establishing a ruleset for responsible release of technologies likely to be abused and embracing and investing in technical privacy solutions. This is especially critical as personal and sensitive private data travel through networks and telecommunications equipment that are highly vulnerable to breaches and surveillance by illiberal governments. Finally—to secure a more open

future—the tech sector must foster and incentivize transparency as the norm within and among private companies.

To build norms that promote digital freedom and incentivize transparency, U.S. tech companies should:

- **Develop guidance for responsible release of novel emerging technologies that are susceptible to abuse (e.g., leverage examples such as Open AI's staged release of GPT-2 language model) to build norms around responsible release.**
- **Continue to advance efforts to safeguard user security and privacy, including through technology such as encryption and other privacy-preserving technologies.** To protect users and avoid transferring individual privacy concerns solely to consumers, companies should continue to invest their engineering capacity in privacy-preserving technologies.
- **Consider publicizing voluntary, biannual public reports on policies and intent regarding data collection, storage, and sharing—if not already doing so.**[42]

Conclusion

The United States should aggressively confront the use of technology that makes "the world safe for autocracy," while preserving individual privacy and liberty.[43] It must create opportunities to harness the digital order for democracy. A privacy moonshot and a federal data protection framework are good starting points. And while our friends are critical in ensuring that democratic values prevail on the world stage, our work starts at home. A comprehensive response must achieve a balance between a one-size-fits-all approach and piecemeal, discrete fixes. Responses from the U.S. government and tech companies alike should avoid adopting the closed or intrusive nature of systems and governance we profess to abhor. The cure cannot be worse than the disease. Instead, the United States must actively reclaim technology for openness and transparency. More individual user control and privacy, more access, more sources of innovation, and more transparency are the new hallmarks of the Shining City. Technology will increasingly reflect the values of our society—let it reflect a free and open one.

The values of a society will be reflected in the way its technology is used. The U.S. government and the tech sector should endeavor to ensure that values of individual liberty, transparency, and openness are imbued in our technology and the laws that govern it.

1. Ely Ratner, Daniel Kliman, Susanna Blume, Rush Doshi, Chris Dougherty, Richard Fontaine, Peter Harrell, Martijn Rasser, Elizabeth Rosenberg, Eric Sayers, Daleep Singh, Paul Scharre, and Loren DeJonge Schulman, "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," (Center for a New American Security, December 2019), https://www.cnas.org/publications/reports/rising-to-the-china-challenge, 24.

2. Sheena Greitens, "The Future of China Studies in the U.S.," ChinaFile, August 27, 2020, https://www.chinafile.com/conversation/future-of-china-studies-us.

3. Martijn Rasser, Elizabeth Rosenberg, and Paul Scharre, "The China Challenge: Strategies for Recalibrating the U.S.-China Tech Relationship," CNAS, December 12, 2019, https://www.cnas.org/publications/commentary/the-china-challenge-1.

4. Some language in these recommendations is derived from the author's September 2020 CNAS publication "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem.

5. Martijn Rasser, Rebecca Arcesati, Shin Oya, Ainikki Riikonen, and Monika Bochert, "Common Code: An Alliance Framework for Democratic Technology Policy," (CNAS, October 21, 2020), https://www.cnas.org/publications/reports/common-code, 1.

6. Ratner et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 26.

7. International Organization for Standardization, "Standards," https://www.iso.org/standards.html.

8. Sui-Lee Wee, "China Uses DNA to Track Its People, With the Help of American Expertise," *The New York Times*, February 21, 2019, https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

9. Quick governance does not always redound to the benefit of citizens or create an environment where innovation can thrive. A centralized, autocratic entity can pass regulations quickly, but alacrity does not ensure that the regulations will be effective or salutary for stakeholders.

10. This framework also addresses threats emanating from malign, foreign actors.

11. U.S. Department of State, *Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, (September 30, 2020), https://www.state.gov/key-topics-bureau-of-democracy-human-rights-and-labor/due-diligence-guidance/; U.S. Department of Commerce, *Bureau of Industry and Security Entity List*, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list; Department of the Treasury Office of Foreign Assets Control, *Global Magnitsky Sanctions Regulations*, 31 C.F.R Part 583 (September 25, 2020), https://home.treasury.gov/system/files/126/glomag_gl2a.pdf; and "Executive Order on Addressing the Threat Posed by TikTok," White House, press release, August 6, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.

12. Derived from the concept of China as a "systemic" rival and competitor—one competing with liberal democracies based on "alternative models of governance"; European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament, the European Council and the Council: EU-China – A strategic outlook," (European Commission, March 12, 2019), https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf, 1.

13. Hence labeling nation states like China "systemic" competitors; European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication to the European Parliament, the European Council and the Council: EU-China – A strategic outlook," 1.

14. Ranking Digital Rights, "2019 Ranking Digital Rights Corporate Accountability Index," (Ranking Digital Rights, 2019), https://rankingdigitalrights.org/index2019/; and Aynne Kokas (Assistant Professor, University of Virginia), in discussion with the author, August 3, 2020.

15. Ratner et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 24.

16. Greitens, "The Future of China Studies in the U.S."

17. Paul Scharre (program director and senior fellow, Technology and National Security Program, CNAS), in discussion with the author, October 20, 2020; and Ratner et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 24.

18. U.S. Department of Commerce, *Bureau of Industry and Security Red Flag Indicators,* https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/51-red-flag-indicators.

19. Scharre, October 20, 2020, discussion.

20. According to the American Enterprise Institute's Hal Brands, "Cost imposition simply refers to the idea of creating friction around an opponent's activities, raising the price that opponent must pay for aggressive behavior, and otherwise imposing a competitive 'tax' on actions that the United States opposes. In competitions that can last for years or decades, cost imposition is fundamental to successful strategy, because even modest costs that are imposed today can compound exponentially over time"; Hal Brands and Tim Nichols, "Special Operations Forces and

Great-Power Competition in the 21st Century," (American Enterprise Institute, August 2020), https://www.aei.org/wp-content/uploads/2020/08/Special-Operations-Forces-and-Great-Power-Competition-in-the-21st-Century.pdf; T. C. Schelling, "The Strategy of Inflicting Cost," in *Issues in Defense Economics*, ed. Roland N. McKean (Cambridge, MA: National Bureau of Economic Research, 1967), https://core.ac.uk/reader/6838278; Hal Brands and Toshi Yoshihara, "How to Wage Political Warfare," *National Interest*, December 16, 2018, https://nationalinterest.org/feature/how-wage-political-warfare-38802; and Hal Brands, "The Dark Art of Political Warfare: A Primer," (AEI, February 6, 2020), https://www.aei.org/research-products/report/the-dark-art-of-political-warfare-a-primer/.

21. U.S. Department of Commerce, *Bureau of Industry and Security Entity List*.

22. Ratner et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 24.

23. Ratner et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 24.

24. Paul Scharre (program director and senior fellow, Technology and National Security Program, CNAS), in discussion with the author, October 19, 2020.

25. Scharre, October 19, 2020, discussion; Sheena Greitens, Associate Professor of Public Affairs at the University of Texas at Austin, testimony to the U.S. Commission on International Religious Freedom, July 22, 2020, https://www.uscirf.gov/sites/default/files/Sheena%20Greitens-%20Uni.%20Texas.pdf, 5. Professor Greitens lays out the first steps in designing such a strategy: "The Bureau of Commerce, the State Department's International Communications and Information Policy Team, and other relevant agencies should craft a strategy that clearly outlines which forums should set standards for which technologies; what those standards and safeguards should be; how interagency efforts should be organized; and how the U.S. should work with allies, partners, and international organizations to collaboratively but assertively shape a global regulatory environment compatible with liberal democracy. Given widespread apparent demand for Chinese surveillance technology, the strategy should consider how to address U.S. concerns over data privacy, democracy, and technological competition while also addressing the legitimate interests of potential recipient countries."

26. "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019," (Government of the United Kingdom, March 2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019, 15–18.

27. Sheena Greitens, "'Surveillance with Chinese Characteristics': The Development & Global Export of Chinese Policing Technology" (paper presented at Princeton University's International Relations Faculty Colloquium, Princeton, New Jersey, October 7, 2019), http://ncgg.princeton.edu/IR%20Colloquium/GreitensSept2019.pdf, 2.

28. Soumitra Dutta, Bruno Lanvin, and Sacha Wunsch-Vincent, "Global Innovation Index 2020," 13th Edition (World Intellectual Property Organization, 2020), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf, xxi, 27, 127, 157.

29. See Section IV "Establish an Affirmative Agenda for Digital Freedom."

30. Ely Ratner, Paul Scharre, and Elizabeth Rosenberg, "Beyond the Trade War: A Competitive Approach to Countering China," *Foreign Affairs*, December 12, 2019, https://www.foreignaffairs.com/articles/united-states/2019-12-12/beyond-trade-war, 6.

31. Rasser, Rosenberg, and Scharre, "The China Challenge: Strategies for Recalibrating the U.S.-China Tech Relationship."

32. Andrew Imbrie, Shanthi Khalil, Aynne Kokas, Alina Polyakova, Laura Rosenberger, Nadia Schadlow, Nicole Wong and others in group discussions with the author, November 2019 to August 2020.

33. Some language in these recommendations is derived from the author's September 2020 CNAS publication "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem."

34. Rasser, Arcesati, Oya, Riikonen, and Bochert, "Common Code: An Alliance Framework for Democratic Technology Policy."

35. Rasser, Arcesati, Oya, Riikonen, and Bochert, "Common Code: An Alliance Framework for Democratic Technology Policy."

36. U.S. Department of Justice, *White Paper on Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, (April 2019), https://www.justice.gov/opa/press-release/file/1153446/download#:~:text=The%20United%20States%20enacted%20the,exploitation%20of%20children%20and%20cybercrime, 2.

37. Ratner et al., "Rising to the China Challenge: Renewing American Competitiveness in the Indo-Pacific," 26.

38. International Organization for Standardization, "Standards," https://www.iso.org/standards.html.

39. "IEEE 7010-2020 Launch Prioritizes Human Well-Being and Environmental Sustainability via Technology," Institute of Electrical and Electronics Engineers, press release, April 30, 2020, https://beyondstandards.ieee.org/tech-ethics/ieee-7010-2020-launch-prioritizes-human-well-being-and-environmental-sustainability-via-technology/.

40. International Organization for Standardization, "Standards," https://www.iso.org/standards.html.

41. Oliver Sachgau and Jackie Simmons, "Siemens Teams With Airbus to IBM in Cyberattack Defense Plan," *Bloomberg Business*, February 16, 2018, https://www.bloomberg.com/news/articles/2018-02-16/siemens-mounts-plan-for-cyberattack-defense-with-airbus-daimler.

42. Chris Sonderby, "Our Continuing Commitment to Transparency," Facebook, press release, May 12, 2020, https://about.fb.com/news/2020/05/transparency-report/.

43. Jessica Chen Weiss, "A World Safe for Autocracy? China's Rise and the Future of Global Politics," *Foreign Affairs*, July/August 2019, https://www.foreignaffairs.com/articles/china/2019-06-11/world-safe-autocracy, 1.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan.

As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, CNAS maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.


Center for a
New American
Security