Stanford | Cyber Policy Center
Freeman Spogli Institute

TOP TECHNOLOGY POLICY PRIORITIES FOR THE NEW ADMINISTRATION

STANFORD UNIVERSITY

Eileen Donahoe

TOP TECHNOLOGY POLICY PRIORITIES FOR THE NEW ADMINISTRATION

Eileen Donahoe of the Cyber Policy Center's Global Digital Policy Incubator argues that the U.S. must rally the world around a democratic, human rights-based vision of digital society, and she recommends a range of early concrete actions that can be taken by the new administration to combat the competing digital authoritarianism model.

The incoming Biden-Harris administration will face many urgent and competing priorities as it seeks to signal a distinct shift from the Trump presidency. In the technology policy realm alone, there are many challenges to confront. Chief among them is the urgent need to solidify international support for a values-based vision of "the internet" and a compelling democratic approach to governance of digital society.

Solidifying an open democratic vision of digital society will require robust diplomacy in three areas. First, we must rebuild global commitment to an open, interoperable, secure and reliable internet and to international norms in the cyber realm. Second, we must lead the development of a shared understanding of what democratic, human rights-based governance of digital society entails. Third, we must bring our democratic allies together around a shared strategic technology agenda.

As context for these efforts, we must start by acknowledging that the original U.S. vision of a global, open, interoperable, internet has been clouded by two big trends: first, heightened anxiety within democracies about the myriad risks associated with connectivity and digitization, and second, perhaps more importantly, competition from a much darker vision of digital authoritarianism.

The digital transformation of society has brought profound change to every aspect of connected society and dramatically altered the context for democratic governance. "The internet" has become the infrastructure

The digital transformation of society has brought profound change to every aspect of connected society and dramatically altered the context for democratic governance.

of society, moving well beyond its early core function of facilitating instantaneously global communication. The wide array of advanced technologies that are now intertwined with all sectors of society has created new vulnerabilities for many aspects of public and private life.

While digitization obviously has yielded substantial benefits, democratic governments are struggling to meet their basic obligations to protect the liberty and security of citizens in this radically changed context. Digitization has created security risks for personal data, confidential communications, and connected infrastructure. Democratic governments are now seized with the fact that digital information platforms have been exploited by malign actors to spread propaganda and disinformation, wreaking havoc on democratic elections and eroding trust in the digital information realm. These threats are testing the ability of democratic governments to protect fundamental freedoms like privacy, free expression, freedom of assembly and association and the right to democratic participation in digitized society. At the same time, the malign actors who have capitalized on these vulnerabilities to attack democracy generally have escaped consequences.

All of this is eroding confidence in democratic governance in the digital realm. The sense of radical insecurity has led some democratic governments to undertake security measures or enact regulations that are inconsistent with their human rights commitments, such as unchecked collection of data in violation of privacy or restrictions for online content that undercut free expression. Furthermore, trust between democratic allies has been eroded by competing assessments of what human rights principles and democratic values actually require in the digital context. In particular, a transatlantic rift

has emerged over a broad portfolio of digital policy challenges, ranging from cross-border data transfers; unchecked digital surveillance by governments; private sector "surveillance capitalism;" monopoly power of U.S. platforms; and tech regulations that fail to conform with democratic values. These digital policy tensions between democratic allies have had the unintended effect of undermining global confidence in the feasibility of adhering to international human rights norms and democratic values in digitized societies.

While democratic governments have been inwardly focused and preoccupied with their own tensions, a digital-authoritarian model of control through data and technology has gained traction globally. This digital authoritarian model, which rests on a concept of "cyber sovereignty," now competes with the open democratic vision of the internet and society. Authoritarian governments, most notably China, have become increasingly adept at using digital technology for repressive purposes at home, role-modeling these practices to the world. They also have capitalized on the growing export-market for surveillance and censorship technologies, spreading these capacities to others to follow their repressive lead.

Unfortunately, China's leadership also recognized earlier than most that dominance in technology brings significant geopolitical, diplomatic and normative influence. Their massive strategic investments in technology already have translated into the ability to embed and spread China's authoritarian values globally, particularly within tech standard and protocol setting bodies like the International Telecommunications Union. Sadly, China's digital authoritarian influence has also shown up in more traditional norm setting arenas, such as the UN Human Rights Council, where absurd declarations of support for China's repressive use of technology in Xinjiang and in Hong Kong have succeeded. Finally, the digital authoritarian concept of "cyber sovereignty," which is antithetical to a global, open, interoperable internet and justifies its fragmentation, also serves as support for a more conventional authoritarian stance — rejection of external criticism based on internationally recognized human rights — now applied in the digital realm.

Strong U.S. leadership is needed to develop a compelling democratic conception of digitized society and to rebuild the democratic alliance around a shared strategic technology agenda.

Democracies must recognize that we are in a geopolitical battle over the governance model that will dominate in the 21st Century digital context. This presents an existential threat not just to U.S. economic and national security, but also to our values-based vision for the internet and open democratic digital society. Strong U.S. leadership is needed to develop a compelling democratic conception of digitized society and to rebuild the democratic alliance around a shared strategic technology agenda.

To achieve these aims, the incoming administration should focus on five practical priorities.

First, we must "get our own house in order" by ensuring that U.S. digital technology policy is consistent with human rights and democratic values. The level of attention to the normative dimensions of technology policy, as well as to investment in emerging technology, must adequately reflect its strategic importance to our security.

Second, the digital policy rift with our transatlantic partners must be healed: without U.S.-EU alignment, other democratic partners will lose confidence that a democratic model for digital society is a realistic goal.

Third, the democratic alliance must be rallied around a shared model for democratic governance of digital society and a strategic technology agenda. This democratic model must incorporate institutional constraints on both public and private sector use of data. It also will require further articulation of how government and technology companies apply and adhere to international human rights law and norms in the digital context.

Fourth, we must compete with the digital authoritarian model of governance and develop a comprehensive strategy to combat it. Robust diplomacy in the international normative arena will be essential, both with respect to technical standards and protocols, and with respect to norms on use of data and technology.

Fifth, the U.S. must reclaim the internet for citizens and humanity by investing in innovation and entrepreneurship in regions that have not been included in the digital revolution, both domestically and internationally. Investment in "E-Government" capacities to provide secure and efficient public services should be uncontroversial, as should investments in digital security tools for citizens, consumers and civil society actors. Expanding access to internet connectivity domestically and abroad should also be an early, uncontroversial priority.

This is a full plate. But early attention to these aspects of the democracy and technology portfolio will pay huge dividends for the Biden-Harris team, the U.S. and the democratic world.

RECOMMENDATIONS FOR THE BIDEN-HARRIS ADMINISTRATION:

I. **Recognize the normative dimensions of digital technology policy as a strategic concern distinct from cybersecurity. Ensure coherence between domestic and foreign policy and adherence to international human rights law and norms.**

Building a democratic approach to digitized society must start at home. U.S. domestic digital technology policy must not undermine our vision of an open internet or our commitment to core human rights principles. "To get our own house in order," we need to assess the use and regulation of data and digital technology by the U.S. government, with reference to fundamental rights to privacy, freedom of expression, and other basic liberties. Accordingly, U.S. policies, applications and regulations related to data, digital platforms, artificial intelligence and other emerging technologies must be evaluated for consistency with human rights principles. Furthermore, the strategic

Building a democratic approach to digitized society must start at home. U.S. domestic digital technology policy must not undermine our vision of an open internet or our commitment to core human rights principles.

importance of technology policy to democracy should be reflected through higher-level coordination across agencies and greater coherence between domestic and foreign policy. The most basic point is that the normative dimensions of technology policy must be seen as a strategic issue and be adequately reflected in both domestic and foreign policy.

The administration should start by strengthening mechanisms for values-based technology policy development and coordination with the United States government.

- **The National Security Council must focus on normative and diplomatic challenges in the digital realm, as distinct from more traditional cybersecurity concerns.** Three focal points include establishing processes to: 1) resolve tensions with allies over how to apply existing international human rights law in the digital context; 2) develop doctrine related to application of international norms in cyberspace related to cross-border harms and malign activity; 3) evaluate human rights impacts of U.S. government use of data and technology across agencies, as well as of the impact of domestic digital technology policies on global internet freedom.
- **The U.S. profile in international technology-related diplomacy must be raised, potentially by establishing an ambassador-at-large for global digital affairs.** The ambassador would elevate U.S. participation in bilateral, multilateral and multi-stakeholder digital and cyber policy development and in international norm-setting arenas. As

a first step, U.S. leadership should be dramatically reinvigorated within the Freedom Online Coalition (FOC), including by seeking to chair the coalition. Robust U.S. diplomacy also is needed at international fora where technology standards and protocols are set, such as the International Telecommunications Union, and in arenas where norms of responsible state behavior in the cyber realm are developed, such as the UN Government Group of Experts. Among the first set of initiatives, the Ambassador could engage the U.S. in the **Paris Call for Trust and Security in Cyberspace.**

- **The new Cyberspace Security and Emerging Technology Bureau at the Department of State announced on Jan. 7, 2021 should be quickly built to serve the goals outlined in the Cyber Diplomacy Act.** The Bureau should cover the full spectrum of technology policy challenges, including development of international norms for cyberspace, tech standard-setting, human rights-based analysis of government and private sector use of data, democratic export controls on technologies of repression, and democratic regulation of digital platforms. The office should take responsibility for developing more robust export controls for repressive technologies and appropriate democratic institutional constraints with respect to government use of data and technologies.

- **Establish a Department of State unit in Silicon Valley, comparable to the Defense Innovation Unit created by the Department of Defense.** Its mandate should include exploration of technology innovations related to more effective use of data and technology in governance and provision of public services, as well as technologies that enhance citizens' privacy, digital security, digital literacy and civic engagement—innovations that the State Departments could then help diffuse worldwide. The office should also be tasked with engaging on policy development with digital platforms and other technology companies, particularly with respect to private sector responsibilities to respect human rights as outlined in the UN Guiding Principles on Business and Human Rights. The unit should also lead in

multi-stakeholder digital policy development processes that bring civil society voices into democratic technology policy development.

II. Resolve the transatlantic digital policy divide, particularly with respect to cross-border data transfers and digital platform regulation.

Any prospect of building a shared democratic technology agenda will require resolution of current tensions between the U.S. and the EU over technology and data. Without U.S.-EU alignment, other democratic partners will lose confidence that a democratic model for digital society is a realistic goal.

Among the most urgent issues to be address are substantial divisions over cross-border data transfer arrangements, digital surveillance by both governments and the private sector, and regulation of digital platforms consistent with democratic values. These disagreements have already **placed** $7 trillion in transatlantic digital trade at risk and led some members of the EU toward a vision of digital sovereignty that could undermine any potential for a shared democratic approach to digital society.

The first step in healing the transatlantic digital policy divide must be an early concerted dialogue with the EU on three priority issues:

- **Rapid development of an alternative to the Privacy Shield data arrangement.** This agreement, negotiated between the U.S. and Europe during the Obama-Biden administration, was struck down in July 2020 by the EU Court of Justice as inconsistent with fundamental rights. Rectifying this problem will require high level negotiations about adequate institutional constraints on government surveillance and appropriate restraints on data-sharing between government and private sector platforms.
- **Agreement on a transparency and accountability regime for digital information platforms applicable to U.S. platforms operating in the EU.** This framework should emphasize users' procedural rights and control of data. Recommendations from

the Transatlantic high level working group **Transparency and Accountability Framework** can provide a starting place. Instead of content-based regulations that place liability on platforms for user-generated content and put freedom of expression at risk, (as seen in some EU country regulations), transparency and accountability mechanisms enhance democratic oversight in ways that are consistent with free expression principles. In addition, greater platform transparency can help educate users, regulators and researchers about algorithmic information systems and build civic resilience to disinformation.

- **A process for resolving conflicting U.S.-EU approaches to fundamental rights in the digital policy realm.** This new process should serve as a vehicle for resolving tensions over conflicting interpretations of how to protect substantive human rights, how to apply international process principles of necessity and proportionality, and how to assess government regulation of digital platforms so that they are consistent with human rights.

III. Galvanize the democratic alliance around a shared values-based vision of digital society and a comprehensive digital technology agenda.

The U.S. should lead a process of renewal for the democratic alliance that inspires optimism and confidence in the superiority of a democratic approach to governance of digital society, as well as commitment to an open internet.

To start the process, the administration should:

- **Capitalize on the opportunity provided by the Summit For Democracy by bringing concerted focus to challenges related to democratic governance of digital society and the strategic importance of values-based digital technology policy for the future of democracy.** The Summit setting will provide a vehicle to jump start the process of developing a more strategic digital technology agenda. It will also provide an early opportunity to help heal democratic divisions over tech regulation, align responses to

tech-related security threats, and expand tech-based partnership. The Summit should cover the full spectrum of technology policy challenges, including strategic tech R&D investment, tech standard-setting, human rights-based analysis of government and private sector use of data, democratic export controls on technologies of repression, democratic regulation of digital platforms, and civic education on responsible use of social media. In addition to policy, a coordinated plan among trusted democratic partners should be initiated to protect the supply chain for essential technologies, such as semiconductors and 5G infrastructure, as well as strategic commitments from democratic partners for increased R&D investments in emerging technologies. Top policy priorities must include development of a mutually beneficial data sharing arrangement among democracies, and shared norms on government surveillance consistent with human rights principles.

- **Following the summit, an ongoing process for developing a shared democratic approach to technology and digital society should be instituted. The process could be divided into different work streams with different "Digital Technology" (DT) partner-groupings:**

  - **DT-10: to develop a strategic technology investment agenda.** Many different configurations are possible. This cohort could be comprised of the U.S., UK, Canada, Australia, France, Germany, Sweden, Finland, South Korea, Japan, plus Taiwan perhaps as an observer-participant. Its primary aim would be to advance a plan to secure supply-chains for critical tech and joint strategic investments in emerging tech.

  - **DT-12: to resolve democratic tensions and seek harmony on digital technology policies.**
    This groups could be comprised of the G7, the EU, Australia, New Zealand, India, and Brazil. Its aim would be to resolve tensions between democratic allies over appropriate checks on government and private sector used of data, as well as harmonious regulatory approaches to private sector platforms.

- **DT+: to defend democratic, human rights-based governance of digital society.**
  This group should include all FOC members (Australia, Austria, Canada, Costa Rica, the Czech Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Ireland, Japan, Kenya, Latvia, Lithuania, the Republic of Maldives, Mexico, Moldova, Mongolia, the Netherlands, New Zealand, Norway, Poland, Spain, Sweden, Switzerland, Tunisia, UK, U.S.), and be open to other democratic allies. The focal point would be to reinforce commitment to freedom in the digital context and to develop a democratic human-rights based approach to governance of digital society.

IV. Combat the emerging digital authoritarian model of governance.

AS the U.S. and our democratic allies struggle to address tensions between ourselves and to reconcile our conflicting digital technology policies, we must not lose sight of the threat posed by authoritarian export of technology and norms. A top priority for the U.S. and our democratic allies must be to develop a comprehensive strategy to combat the rise of digital authoritarianism. To this end, the U.S. must:

- Renew global advocacy for a free and open internet with an updated vision for how to protect it.
  - **Rejoin the UN Human Rights Council (HRC) to rebuild the global normative consensus around internet freedom.**
    The U.S. should lead in developing an advocacy strategy to counter authoritarian influence at norm setting bodies and normalization of authoritarian applications of digital technology that violate human rights.
  - **Invest in coordinated international diplomacy at multilateral and multi-stakeholder fora where technology standards and protocols are developed.**

- **Resist export of authoritarian digital information infrastructure and support a stronger export control regime for authoritarian surveillance and censorship tools.**
  - In particular, restrict China's access to technology and equipment that facilitates domestic semiconductor manufacturing.
- **Prioritize development of civic resilience to cross-border information operations and the spread of propaganda and disinformation by authoritarian governments.** Rebuilding trust in information will be essential for civic engagement in democratic digital society. To date, democratic governments have been inadequately prepared to combat these challenges and need significant improvements to stay ahead of adversaries.
  - **Build a multistakeholder mechanism for developing best practices to combat disinformation,** modeled on the Global Internet Forum to Counter Terrorism (GIFCT), including a vehicle for information-sharing between government, civil society, the research community and the private sector.
  - **Build stronger transnational information sharing mechanisms between democratic allies,** to counter foreign malign information operations and share best practices in building civic resilience.
  - **Advocate for new norms for professional reporting on hacked material and disinformation,** as proposed in the Stanford Guidelines for reporting on disinformation and hacked material
  - **Increase investments in building civic resilience to digital disinformation, including public education on norms of civic discourse, media literacy and digital literacy.**
  - **Advocate for the Transatlantic Commission on Election integrity** Election Pledge to strengthen norms and expectations for political candidates and parties to reject and denounce propagation of disinformation around elections.

V. Reclaim digital technology for civil society and humanity.

To rally the democratic world around a democratic vision of digital society, the U.S. must help restore a positive vision of how technology can support democratic activity, civic engagement and the enjoyment of human rights. The new administration should invest in innovation and access to technology to empower citizens. To this end, the U.S. should:

- **Support development of artificial intelligence (AI) applications to achieve the Sustainable Development Goals,** while respecting the right to equal protection and nondiscrimination by ensuring inclusion in the benefits of AI; the data used to feed AI; the coding community that builds AI; and in AI policymaking.
- **Role-model inclusivity in the U.S. domestic context, by pledging to provide Internet access for all Americans,** with particular focus on access for minorities, vulnerable communities, women, and economically disenfranchised citizens. Invest in rural and urban broadband in unserved areas, commit to ensure internet connectivity across the U.S., and advocate for universal internet access internationally.
- **Provide digital security education and tools for U.S. citizens and global civil society** and funding for digital and media literacy education and **create a fund to invest in emerging technologies to support and encourage civic participation.**
- **Invest in "E-government" technology innovations that enhance efficiency, security and accountability in government provision of public services.** Explore the use of public data trusts, secure digital ID, and technology platforms that enhance citizen communication with elected representatives.

- **Support global technology innovation and entrepreneurship particularly in the Global South.** A genuinely inclusive and democracy-sustaining global internet must entail some "home-grown" digital platforms and services emerging in the developing world, especially in countries where internet adoption is growing fastest.

ABOUT THE AUTHOR

Eileen Donahoe is the Executive Director of the Global Digital Policy Incubator at Stanford's Cyber Policy Center. She served as U.S. Ambassador to the UN Human Rights Council during the Obama administration, and then as Director of Global Affairs at Human Rights Watch.