Stanford | Global Digital Policy Incubator
Cyber Policy Center

A Rights-Respecting Digital Policy Agenda:

Human Rights Community Perspectives for the New U.S. Administration

January 2021

Kip Wainscott | Megan Metzger | Tracy Navichoque | Mackenzie Austin | Eileen Donahoe

Stanford | Global Digital Policy Incubator
Cyber Policy Center

A Rights-Respecting Digital Policy Agenda:
Human Rights Community Perspectives for the New U.S. Administration

Table of Contents

Overview

In the months leading up to the U.S. presidential election, the Global Digital Policy Incubator undertook a discovery project to illuminate potential opportunities in the new administration to advance a rights-respecting digital policy agenda. This project was motivated principally by awareness that the rights community is often underrepresented within formal government planning and transition processes.

To elucidate perspectives from these important stakeholders, our team conducted interviews with human and digital rights experts, capturing reflections across the following five topic areas:

- **Platform Accountability and Information Integrity**
- **Digital Privacy and Security**
- **Government Regulation of AI and Machine Learning**
- **Technology Access, Infrastructure, and Skills**
- **Countering Digital Authoritarianism**

This report synthesizes the experts' commentary and provides summaries of their recommendations for advocates, policy professionals, and government appointees working to elevate rights considerations in the digital policy context.

Summary of Recommendations

At a high-level, the recommendations fell into the following four types:

1. **Strategic recommendations:** Strategic proposals to advance a rights-respecting digital policy agenda included improving coordination with democratic allies, elevating digital policy priorities within multilateral fora, and ensuring that domestic digital policies align with the principles of a free and open internet and other tenets of America's foreign policy in the digital realm.

2. **Policy recommendations:** Recommendations included a comprehensive consumer data privacy framework as well as transparency and auditability standards for digital platforms and emerging technologies. These recommendations consistently prioritized the development of domestic policies that reflect democratic values and model democratic governance of digital society.

3. **Societal investments:** Proposals included expanding support for civil society and educators' efforts to promote digital literacy; investing in secure cyber infrastructure; and ensuring universal, affordable broadband access throughout the United States in order to strengthen civic resilience, promote accountability, and expand access to technologies that facilitate the exercise of rights.

4. **Organizational and structural recommendations:** Recommendations included the creation of new functions and offices to lead and coordinate digital priorities, as well as efforts to better integrate technologists and other relevant experts into the policy development processes.

Cross-Cutting Themes

Two cross-cutting themes emerged throughout the consultations as relevant across all policy topics:

- **The new administration must take steps to ensure the domestic tech policy agenda is coordinated with the nation's foreign policy objectives.** Digital policies have global implications, particularly when implemented in the United States, which is home to many of the world's most popular digital platforms.

- **The United States' digital policy agenda should be coordinated multilaterally.** By coordinating digital policy priorities among allies, democratic nations can advance a global, values-based framework for technology governance and digital rights––amplifying pressure on technology companies to adhere to these shared values, and giving users a clearer choice

between a rights-respecting digital model and technologies that reject (or decline to embrace) such values.

Methodology and Approach

Experts were invited to participate in this project based on their demonstrated contributions to the field of human rights and digital policy. Given this project's focus on actionable advice for U.S. government stakeholders, the experts consulted were either located within the United States or have experience engaging with U.S. policy issues.

Each expert participated in a 45-minute interview with the expectation that their commentary was not for attribution. Their inputs have been synthesized and anonymized as part of these summaries. However, the experts below granted GDPi permission to note their participation. We value their contributions to this project and are appreciative of their time.

Participating Experts

- **Aaina Agarwal**, *International Policy & Human Rights Advisor, Algorithmic Justice League*
- **Matt Bailey**, *Program Director, Digital Freedom at Pen America*
- **Charles Bradley**, *Executive Director, Global Partners Digital*
- **Jennifer Brody**, *AccessNow*
- **Andrew Crocker**, *Electronic Frontier Foundation*
- **Steven Feldstein**, *Senior Fellow, Carnegie Endowment for International Peace*
- **Gennie Gebhart**, *Electronic Frontier Foundation*
- **Sam Gregory**, *Program Director, Witness*
- **Neema Singh Guliani**, *Former Legislative Counsel at the American Civil Liberties Union*
- **Brittan Heller**, *Technology & Human Rights Lawyer, Foley Hoag LLP*
- **Sabrina Hersi Issa**, *Human Rights Technologist & CEO of BeBold Media*
- **David Kaye**, *UC Irvine School of Law and former United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*
- **Mark Latonero**, *Fellow, Harvard Kennedy School's Carr Center for Human Rights Policy*
- **Emma Llansó**, *Director, Free Expression Project at the Center for Democracy and Technology*
- **Rebecca MacKinnon**, *Founding Director of Ranking Digital Rights*
- **Nicholas Miller**, *International Center for Not-for-Profit Law*
- **Elizabeth Renieris**, *Berkman Klein Center for Internet & Society, Harvard University*
- **Matt Stempeck**, *Civic Technologist*
- **Amy Studdart**, *Digital Democracy at the International Republican Institute*
- **Dr. Claire Wardle**, *Executive Director, First Draft*
- **Chris Worman**, *Vice President for Alliances and Program Development, TechSoup*
- **Vera Zakem**, *Senior Technology and Policy Advisor, Technology for Global Security*

Topic Areas and Recommendations

Platform Accountability and Information Integrity

Topic Overview

Our consultations touched on an expansive range of policy challenges and considerations related to improving Platform Accountability and Information Integrity. Experts consistently highlighted challenges for governments and private sector platforms in addressing harmful online content without undermining core commitments to freedom of expression. In particular, the spread of digital disinformation threatens the quality of civic discourse broadly, and around elections specifically, with bearing on multiple aspects of freedom of expression, such as access to information, the right to form opinions, and the right to political participation. In addition, the effects of online hate speech can chill expression and contribute to offline harms and violence, posing particular risks to vulnerable communities.

Experts also expressed concerns related to the lack of transparency required of large digital platforms and the inadequacy of accountability mechanisms, particularly with respect to changes to and the application of platform rules, algorithmic curation of information, and user complaint procedures. In discussing issues of accountability, topics such as competition and antitrust; data transparency and auditability; and user rights were recurring themes. Similar to efforts to advance information integrity, policies related to accountability and liability were noted to carry important implications for free expression and access to information, as well as for freedom of assembly, privacy rights, and the rights to health and security.

Recommendations for the new US Administration

Our consultations yielded the following recommendations for advancing platform accountability and information integrity.

1. **Create a senior position at the White House that serves as an interagency nexus on a platform accountability.** The administration should not segment the platform accountability agenda into discrete siloes (for example, with one team dedicated exclusively to tech competition and another working solely on digital privacy). There must be a holistic all-of-government approach to democracy-compatible internet policy and digital platform accountability. A more holistic approach will help ensure that policies crafted for one purpose, such as ensuring competition, do not have unintended consequences for other policy objectives or the country's global internet freedom agenda.

2. **Advance corporate transparency practices and mechanisms for accessing data from platforms.** The U.S. administration is encouraged to move away from a piecemeal approach to content-based platform policy and instead undertake the development of transparency standards that facilitate a meaningful, rights-

respecting exchange of information. These standards should empower users with information regarding platform content policies, enforcement practices, and data collection.

3. **Rebuild trust and re-envision the relationship between technology and society by developing policies and mechanisms to hold companies accountable for abuses and failures.** An expert noted that "the lack of trust on the internet and in relation to tech and platforms contributes to so many challenges and cuts against issues in all directions. . ." To rebuild and regain trust, the U.S. government must present a model for accountability, which may include authorizing regulatory auditing mechanisms, repealing Executive Orders that undermine a free and open internet, and developing processes for users to vindicate privacy rights vis-à-vis large platforms.

4. **Bridge the knowledge differential between policymakers and industry stakeholders by bringing technology expertise to government.** Rights experts lament that policymakers are often not appropriately versed on technology matters to develop creative policy solutions or informed judgments regarding platform activities. To help promote informed policy development and lawmaking, the new administration should not only invest in strategies to recruit tech talent to the executive branch, but also support congressional efforts to reestablish the Office of Technology Assessment.

5. **Enact comprehensive federal privacy and consumer privacy legislation.** Without a guarantee of privacy, users may fear surveillance and self-censor as a result. Privacy vulnerabilities may chill speech and also endanger an individual's information without consent. In addition, the malicious use of private information can be weaponized against internet users as part of what the digital rights community refers to as "mal-information" campaigns. Efforts to regulate digital platforms through changes to content and liability laws should not undermine digital privacy rights or weaken encryption standards.

6. **Reinvest in multistakeholder digital policy development.** A global internet requires a global multilayered conversation. Internet sovereignty is chipping away at the fabric of a global and shared internet. With each country or region setting their own standards, the issue of incompatible policy agendas becomes more prominent. Global conversations about the internet should entail both multilateral and multistakeholder processes.

Operational Steps

These policy issues can be deceptively nuanced and require far greater delicacy than the public debates might suggest. While, for example, there is broad political support for improving platform accountability, calibrating and building support for specific proposals such as liability expansions, competition, or content regulation will require heavy lifting.

In light of the complexities, one expert recommended that policy leaders in a U.S. administration be intentional about framing this agenda in the context of rights and freedoms. "If there's any hope of advancing an agenda that won't descend into partisan squabbling, [the administration] has to define this in terms of freedom of expression and... champion [it]." This kind of intentional framing and discipline was also recommended as a means of ensuring focus on these issues, despite other urgent priorities that a U.S. administration will need to balance in 2021.

Policymakers should be cognizant of how digital platforms may be positioned to leverage their knowledge and information advantage in the context of lobbying. Recruiting technical knowledge into the policymaking ranks and engaging external knowledge through multi-stakeholder processes will be essential to help mitigate these dynamics.

Digital Privacy and Security

Topic Overview

Digital privacy and security are foundational to protecting rights and freedoms in the digital realm. Concerns in this space relate to both government surveillance and security threats, as well as risks in the commercial context of consumer privacy and surveillance capitalism. Data privacy concerns extend to nearly every facet of life, from health information and biometric identifiers to banking and financial information and locational data. This expansive domain warrants careful attention from policymakers.

Digital privacy and security challenges implicate a range of human rights, including freedom of assembly and movement, due process rights, and the right to privacy. As one expert noted, "It's not only the *knowledge* that you might be surveilled online that chills speech and makes you think twice about what you say, it's the fear or uncertainty that it's possible you are being surveilled."

Recommendations for the new US Administration

Our consultations yielded the following recommendations for advancing digital privacy and security.

1. **Prioritize development of a long-term, comprehensive strategy that elevates digital privacy and security.** The new administration should develop a strategic framework clarifying standards and objectives that can be referenced across multiple policy contexts. This would include executive branch policies regarding federal agencies' collection, use, and storage of data; multilateral negotiations regarding international data sharing practices; and legislative negotiations regarding both consumer privacy rights and government surveillance authorities. This framework should elevate civil rights and human rights considerations of new technologies and require a review of existing privacy laws and policies (both consumer-facing and government-facing) to identify any gaps or vulnerabilities.

Policymakers should move beyond the existing consent-based approach to privacy, which places responsibilities on users, and instead set clearer expectations as to the responsibilities of entities collecting data.

2. **Assert American leadership in the development of international standards for privacy and cybersecurity.** The recent European Court of Justice (CJEU) decision in *Schrems II* underscored the importance of international coordination in the protection of digital privacy rights. As one expert emphasized, "one of the most immediate considerations for a new administration will be to determine how to engage the European Union in the aftermath of *Schrems II* . . . the U.S. must have a strategy for these international dynamics." The new administration should promote and protect privacy rights in the international context, including attention to negotiating international data transfer standards, mutual legal assistance treaties, and other international authorities such as CLOUD Act agreements.

3. **Develop and implement comprehensive policies for federal agency collection and use of remote biometric identifiers and the application of AI-powered technologies.** Biometric identification through facial recognition technologies, for example, represent a growing risk in the context of government surveillance. The new administration should develop policies that are grounded in human rights, clarify the circumstances under which federal agencies can use such technologies, and appropriately account for the risks to privacy and civil liberties these technologies pose. "Human rights, such as rights to life, liberty, security, privacy, and expression, should be at the center of the debate for emerging technologies including artificial intelligence-powered systems and tools," stated one expert.

4. **Leverage expertise and improve oversight to advance and protect digital security and privacy priorities.** Citing the diminished ranks currently across the civil service, experts encouraged the new U.S. administration to leverage outside knowledge––particularly the expertise of civil society––while concurrently investing in programs and initiatives to recruit talent into government, which should include reinvigorating the U.S. Digital Service. The administration should empower relevant civil rights and civil liberties components within various agencies to contribute more substantially to the development of digital policies and data governance practices. Moreover, the new administration should build stronger oversight capacity and work with Congress to fund a federal data protection regulatory authority "with the ability to invalidate data transfer mechanisms … localization mechanisms and … look at cross-border impacts and risks."

5. **Promote digital privacy and security through public awareness and education.** Digital literacy and training investments are key to building a future in which citizens can ably protect their rights. These public education strategies should be approached as a long-term multi-decade investment to build awareness among Americans as to how to protect their privacy.

Operational Steps

Policymakers should be especially aware of two operational dynamics. The first is the classic tension between privacy and security equities within government. Many government stakeholders––including law enforcement, intelligence, national security, and immigration authorities––are conditioned to favor what one expert called a "collect it all" approach to data, to either fulfill their agency mission or protect security and safety. While experts perceived this orientation to be deeply-rooted, they also expressed confidence that it would not be insurmountable. The development of a comprehensive strategy can help promote a sense of common purpose.

The second consideration is that certain government agencies are now accustomed to leveraging private sector data collection in support of their missions. This dynamic contributes to friction around efforts to curtail surveillance capitalism and implement stricter privacy standards in the commercial sector.

As one expert put it, private sector tools are often outpacing government in terms of sophistication and analytical power. Policymakers must overcome institutional temptations to permit expansive private sector data collection that bypasses the legal process. Policy models from other domains, such as global financial regulations, may hold lessons for building interoperable frameworks that are responsive to cross-border flows of data.

Finally, the applicability of international human rights frameworks is an underappreciated and underdeveloped resource for policymakers thinking about digital privacy and security. These frameworks are imperfect, but they are "the closest thing we have to a global consensus."

Government Regulation of AI and Machine Learning

Topic Overview

Artificial intelligence and machine learning (AI/ML) include a broad range of technologies, requiring varied regulatory approaches. Many AI/ML technologies already impact people's lives, particularly automated surveillance technologies, algorithmic decision-making in the criminal justice system (for example in pre-trial release), and the use of facial recognition by law enforcement. Conversations on these topics often get derailed by emerging technologies, while issues related to technologies already in widespread use have yet to be fully addressed. For example, experts noted that a larger amount of public focus has centered on the potential harm of political deep fakes, when the most common existing harm from these technologies comes in the context of non-consensual pornographic depictions of women.

Recommendations for the new US Administration

Our consultations yielded the following recommendations on the government regulation of AI and machine learning.

1. **Develop a clear strategy for the governance of AI and machine learning, grounded in human rights**. The number one recommendation of almost all experts on this topic is to develop and implement a clear strategy and process for how regulatory questions about AI will be approached, before tackling any single regulatory question in particular. As one expert noted, there can be "a tendency to...move piecemeal [in this space] and that…[can] end up being counterproductive to ultimately securing human rights aims in the policy initiatives that move forward." There is a real risk of suboptimal policy outcomes when decisions are made without clear, rights-oriented processes in place. Additionally, effective strategy and processes can help ensure better regulation even as uses of AI advance.

2. **Prioritize the inclusion of diverse voices, particularly from vulnerable groups and those most impacted by AI and machine learning technologies.** Current governance approaches often focus on the impacts that are most visible to outside observers, but this may not adequately capture the real impacts on those whose liberty may hang in the balance of AI-informed decisions. Developing a truly inclusive process is a challenge, and for this reason it's important for a new administration to make this an early priority.

3. **Focus regulation on technologies that are already deployed and that risk substantial real-world harms.** Many technologies that are already in use have the potential to cause substantial real-world harms and these should be prioritized. For example, regulating the use of facial recognition by law enforcement and the use of algorithms in the criminal justice system should be an early focal point. Research has suggested that both of these uses can contribute to amplifying existing racial and other biases in the criminal justice system. The new administration should begin by using a well-defined process to focus their regulatory attention on the harms already occurring, and then expand that regulation as new technologies or uses emerge.

4. **Recognize that regulation of AI and machine learning is a global challenge.** Cooperation with allies is necessary to ensure rights-respecting approaches to these technologies at home and abroad. The new administration should apply pressure internationally to limit the use of AI for repressive purposes and make sure that U.S. companies are not using AI/ML tools in ways that threaten human rights. The administration should ensure that surveillance tools produced by U.S. companies are not sold or licensed without an assessment of the potential risks for

repression. Multilateral collaboration is critical, given that technologies built in one country can easily proliferate to others.

5. **Avoid over-reliance on newly emergent "ethics" or "ethical principles."** Some experts expressed skepticism about the range of recent AI "ethics" or "ethical principles" because they elevate certain aspects of human rights, such as privacy, while failing to fully engage with the full range of obligations. The different frameworks can also contribute to confusion around how to approach the regulation of AI. Instead, the human rights framework provides a better global foundation for assessing AI/ML tools and applications, as well as AI/ML regulation.

Operational Steps

The new administration should coordinate an all-of-government approach to AI/ML. The creation of a national artificial intelligence strategy as well as a high-level committee or interagency task force are two potential approaches to ensure cross-government cooperation. Regulatory decisions should be based on best practices and current knowledge in this space. The new administration should designate a point person on AI that regularly communicates with senior leadership.

Moreover, all government research and procurement should engage in human rights due diligence. There should be mandatory human rights impact assessments for any projects receiving government funding (for example from the NSF, USAID, DARPA, etc.), and that any technology used by the government itself be required to agree to standards that consider rights at every step of the process.

Economic and other incentives towards innovation should not stymie progress on much needed regulation of AI and machine learning-based technologies in the United States. The new administration should argue that responsible innovation can also be economically feasible. In the long term a rights-respecting approach to AI will be a competitive advantage.

Technology Access, Infrastructure, and Training

Topic Overview

Issues related to Technology Access, Infrastructure, and Training were among the most cross-cutting of the topics our interviews explored. This policy area covers advancing digital opportunity among American citizens and workers, and building capacities to improve the government's ability to responsibly navigate the digital age. It includes both specific policy recommendations (such as net neutrality, and digital identity), as well as important structural priorities, such as investing in skills and knowledge, and developing mechanisms that promote accountability and oversight of digital services and data practices. Access and education initiatives can help to build resilience to a broader range of digital risks to rights such as privacy and free expression.

Internet accessibility directly impacts the right to access information, which has broad implications for free expression, political participation, and other rights. Internet accessibility and technology infrastructure also intersects with equity and justice issues like in the context of health and educational rights. Risks to rights are particularly acute in the context of the COVID-19 pandemic, as we have been forced to reevaluate our relationship with online activity and social media platforms and have become even more aware of inequities as the world has moved further online.

Recommendations for a US Administration

An agenda to strengthen U.S. technology access, infrastructure, and training should build from the following recommendations:

1. **Ensure internet access for all communities.** The U.S. government should expand connectivity through a range of measures and approach the issue of access to the internet as a right, not merely a commodity. These initiatives should ensure access to affordable internet service in a fast and reliable way irrespective of where Americans live. In support of promoting equitable access, the new administration should recommit to the principles of net neutrality and consider oversight mechanisms to ensure that telecommunications companies are serving "last mile" communities.

2. **Promote digital literacy and reimagine digital workforce training.** There should be a paradigm shift in education that enables communities to continuously learn relevant digital and technical skills. In support of this vision, experts called for the incoming administration to advance federal workforce training and establish what one expert characterized as a "digital AmeriCorps," a large-scale program that acquaints Americans with the fundamentals of internet architecture. Digital literacy would not only equip people with skills for employment, but would also lead to a better understanding of privacy and digital rights.

3. **Prioritize investment in digital infrastructure and strengthening technology capacities throughout government**. Invest in public sector technologies and government competencies to build a more equitable digital future in the U.S. The new administration should undergo a comprehensive assessment of current U.S. digital capacities to identify areas of weakness. As one expert put it, "to build a new house you need a strong foundation, and capacity in places like the Office of Science and Technology Policy have been eroded and systematically dismantled in recent years." The administration should secure national connectivity infrastructure and develop strategies for modernizing digital governance capacities, including advancements in digital identification.

4. **Practice public accountability.** Eroding trust in both government and technology has become a significant liability for U.S. democracy. To help bridge this trust deficit, experts recommended that a U.S. administration take steps to promote

greater transparency and accountability with respect to the government's own use of data and technology, by:

- Developing efficient channels for the public to seek information about their data and resources in the event of a breach or other cyber incident with implications for citizens' privacy. Many experts cited Estonia as a potential model (or, as one expert described it, "FEMA, but for data challenges").
- Making federal data more accessible, by curating and opening privacy-respecting federal datasets, and creating opportunities for the public to understand and make use of the data. These steps should be taken in conjunction with the launch of a national data trust, into which federal agencies and civil society organizations who accept federal funding can also contribute datasets.
- Appointing a civil society ombudsman to assess public data stewardship.

Operational Steps

The scale and long-term nature of this work doesn't lend itself to notching "a sexy win" for political purposes. Asked about headwinds facing this agenda, one expert explained, "it's hard for long-term infrastructure goals to compete with immediate priorities like employment."

As the pandemic has underscored the urgency around connectivity, experts recommend integrating relevant elements of this agenda into pandemic response initiatives to ensure they are appropriately prioritized. Ireland and Australia may illustrate the ways that digital capacity can be elevated as part of COVID-19 recovery efforts.

Regarding connectivity and accessibility objectives in particular, the new administration should also be mindful of entrenched private sector interests related to these issues. For example, current regulatory conditions have created environments in which some communities lack competition, and thus go unserved. Officials should anticipate that the telecommunications industry will be resistant to changes that may enable greater competition. The new administration should approach these structural-level technology issues as part of a wider mission to **restore trust** in the United States.

Countering Digital Authoritarianism

Topic Overview

Countering digital authoritarianism was ranked as an important priority for the new administration, not only because of threats presented to global stability and international human rights, but also the risks to Americans' rights and national security.

The global trend toward digital authoritarianism entails the increasingly widespread use of digital technologies by authoritarians for repression at home, through surveillance, censorship and information manipulation; the export of technologies of repression

abroad for these same purposes; and sophisticated international diplomatic efforts to undermine global commitment to human rights in digitized society.

Among the primary human rights threatened by digital authoritarianism are the rights to privacy, freedom of expression and freedoms of assembly and movement. As both an instrument of oppression and an economic tool, widespread surveillance coupled with the integration of various data sets substantially diminishes the rights, humanity and autonomy of citizens, in part by substituting choice and decision-making with rote analytics.

Recommendations for a US Administration

1. **Connect efforts to counter digital authoritarianism more explicitly to the human rights framework.** Policies to counter digital authoritarianism should be grounded explicitly in the human rights framework to reinforce the relevance of human rights to national security and geopolitics. The new administration should make clear that digital oppression jeopardizes human rights.

2. **Clarify and elevate concerns about digital authoritarianism in multilateral fora.** Lack of definitional clarity or consistency in what is included in the digital authoritarian threat landscape is a barrier to progress. The U.S. should elevate these challenges within multilateral fora and develop new multilateral platforms or coalitions.

3. **Improve interagency coordination and structural organization.** Countering digital authoritarianism and advancing internet freedom implicate an expansive number of policy issues, many of which are managed across multiple federal agencies. Progress on these issues has suffered from a lack of coordination and information-sharing. The new administration should update interagency processes to connect workstreams and empower a high-level official to facilitate coordination across the government.

4. **Build resilience by investing in civil society and efforts to strengthen democratic institutions.** The new administration should increase support for civil society organizations working to build resilience to digital authoritarianism. This might include strengthening independent journalism, promoting programming for digital literacy, prioritizing government transparency, and centering inclusive political participation.

5. **Present an alternative democratic vision for digital norms and practices.** To counter digital authoritarianism effectively, the U.S. must be capable of articulating a compelling alternative vision for a free and open digital future.

Operational Steps

While digital authoritarianism is an emerging concept, authoritarian governance has long laid the groundwork for its spread. Therefore, rebuilding the democratic alliance around a shared vision remains an effective bulwark against the abuse of power on and offline.

Digital authoritarians have used the international system to bend standards towards their agendas. As a result, digital repression efforts must be countered in the multilateral sphere with international coordination.

The State Department should increase support for a global internet forum focused on countering digital authoritarianism, drawing on expertise within the Office of Science and Tech Policy, and revitalize the Bureau of International Organization Affairs. These steps create a foundation of strength that the US government can work from to tackle the challenges posed by this global threat.

The new administration must also “incorporate smart external thinking” by bringing in expert technologists into the policy making area. Policies will also need to include public investment in research and development that positions the United States to maintain technological competitiveness. Moreover, the administration should ensure that domestic tech policies reflect the United States’ respect for privacy, digital rights, and human agency.