February 26, 2024

The Honorable Antony J. Blinken
U.S. Department of State
2201 C Street N.W.
Washington, D.C. 20520

The Honorable Gina M. Raimondo
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

The Honorable Katherine Tai
Office of the United States Trade Representative
600 17th Street NW
Washington, DC 20508

Dear Secretaries Blinken and Raimondo and Ambassador Tai:

The below-signed civil rights, civil liberties, and open Internet advocates have championed a free and open internet while fighting against the harms that emerging technologies may pose for liberty, privacy, and equity. These goals can – and must – be achieved together. While we appreciate President Biden's steps to address the actual and emerging harms of artificial intelligence,[1] we are concerned that the withdrawal of key commitments at the World Trade Organization and in international trade negotiations will signal that the United States no longer stands by a free and open internet. We ask that you reiterate the United States' twin commitments to preserving the internet as a truly global medium and to retaining its ability to make specific adjustments to allow for critical public policy objectives such as the regulation of algorithmic systems to support privacy and equity.

Late last year, the U.S. Trade Representative withdrew support for a number of commitments at the World Trade Organization that underpin a global, open internet,[2] including opposing forced data localization, supporting the free flow of information, combatting mandatory transfers of intellectual property, and championing non-discrimination for information products.[3] Advocates and governmental bodies have long championed these commitments as key for fostering human rights and ensuring access to information globally.[4] As former Federal Communications

[1] *E.g.*, Comments of the American Civil Liberties Union, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, Docket No. OMB-2023-0020 (Dec. 5, 2023), here; Comments of the Center for Democracy & Technology (Dec. 5, 2023), here; ReNika Moore & Cody Venzke, *ACLU Statement on President Biden's Executive Order on Artificial Intelligence*, ACLU (Oct. 30, 2023), here.
[2] Gavin Bade, *NSC, USTR at Odds Over Digital Trade Decision at WTO*, Politico Pro (Nov. 9, 2023), here.
[3] Letter from Sens. Ron Wyden, Mike Crapo et al. to President Joseph R. Biden (Nov. 30, 2023), here (hereinafter Congressional Letter).
[4] Adrian Shahbaz, Allie Funk & Andrea Hackl, *User Privacy or Cyber Sovereignty? The Human Rights Implications of Data Localization*, Freedom House (July 2020); *Policy Brief: Human Rights*, Internet Society (Oct. 30, 2015),

Commissioner Michael Copps observed in early net neutrality debates over two decades ago, these commitments reflect the recognition that "Internet openness and freedom are threatened whenever someone holds a choke-point that they have a legal right to squeeze. That choke-point can be too much power over the infrastructure needed to access the Internet. And it can also be the power to discriminate over what web sites people visit or what technologies they use."[5] Those concerns apply whether the discriminatory power is exercised by private power or public authorities.

The United States' withdrawal of its commitments may be read to signal an abandonment of those principles of openness, freedom, and non-discrimination:

- **Data localization.** Data localization requirements may be abused to disfavor foreign companies and speakers and undermine the functioning of a global, interoperable internet by upending the ways in which data can flow across borders.[6] Data localization places personal data "firmly within reach of governments,"[7] creating unique risks for people's privacy, free expression, access to information, and other fundamental freedoms.[8] Data localization efforts can also exacerbate cybersecurity concerns by requiring duplication of the servers and data localized in each jurisdiction.[9] Those cybersecurity vulnerabilities may make data *more* vulnerable to foreign surveillance and privacy breaches, while failing to address sophisticated attacks that do not rely on the foreign transfer of data.[10]
- **Restrictions on cross-border flows of information.** International flows of information are essential for people in the United States and around the world to participate in global discourse and commerce, and broad limitations on those data flows would restrict their ability to access content from across the globe.
- **Forced disclosure of source code.** The forced disclosure of products' source code may undermine intellectual property rights, privacy, and security. An entity that is required to disclose source code "may fear theft of its IP" and its transfer to a competing entity.[11] Mandated disclosure of source code may likewise allow adversaries to identify and exploit security and privacy vulnerabilities. Although the United States should commit to protecting against forced transfers and exploitation of source code, those commitments

---

here; Sen. Ron Wyden, *The Free Internet Is a Global Priority*, Wired (Apr. 22, 2015), here; *The Impact of Forced Data Localization on Fundamental Human Rights*, Access Now (June 4, 2014), here.

[5] Michael J. Copps, Commissioner, Federal Communications Commission, Remarks at New America Foundation at 9 (Oct. 9, 2003), here.

[6] Shayerah I. Akhtar & Michael D. Sutherland, Congressional Research Service, Digital Trade and U.S. Trade Policy 15-16 (2021), here (hereinafter CRS Report).

[7] Erol Yayboke et al., *The Real National Security Concerns over Data Localization*, CSIS (July 23, 2021), here.

[8] Allie Funk & Jennifer Brody, *Reversal of US Trade Policy Threatens the Free and Open Internet*¸ Tech Policy Press (Nov. 14, 2023), here.

[9] H Jacqueline Brehmer, Data Localization: The Unintended Consequences of Privacy Litigation, 67 Am. U. L. Rev. 927, 962-63 (2018), here.

[10] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 714-21 (2015), here.

[11] CRS Report at 17-19.

should still permit sufficient transparency around algorithmic systems to guard against discrimination and other harms, as discussed below.

- **Discrimination against foreign digital products.** Nondiscrimination has long been a keystone in U.S. digital policy, ensuring that individuals, not governments or infrastructure providers, ultimately choose what information is created and accessed.[12] This principle enables individuals to choose the best products and platforms for their needs – including those that have better content moderation or privacy policies.

Abandoning those commitments can result in concrete harms. For example, data localization mandates might impact a global service like Wikipedia (the free online encyclopedia created and maintained by volunteers around the world) and its users worldwide. Over the past decade, the Wikimedia Foundation (the nonprofit that hosts Wikipedia) has received an increasing number of requests to provide user data to governments and wealthy individuals, who wish to censor accurate public information or to identify and take retaliatory action against the volunteers editing Wikipedia.[13] These mandates would worsen this trend by subjecting the data of vulnerable individuals to direct seizure by authorities that do not respect human rights.

Besides threats to privacy, free expression, and even the safety of Wikipedia volunteer editors, the financial costs of establishing data collection and storage facilities in countries around the world would threaten the economic viability of nonprofit, small businesses, and larger commercial entities alike.

Growing requirements for data localization are happening alongside a global crackdown on free expression. And people's personal data – which can reveal who they voted for, who they worship, and who they love – can help facilitate this. Rwanda's data protection law, for instance, mandates that companies store data locally unless the country's non-independent cybersecurity regulator approves otherwise. This requirement leaves personal data easily accessible in an environment in which authorities have embedded agents in telecommunications companies and used data from private messages to prosecute dissidents.[14] Similarly, in Uzbekistan, authorities temporarily blocked Skype, TikTok, Twitter, VKontakte, WeChat, and other popular platforms due to their noncompliance with a data localization law, severely limiting people's ability to communicate and access information.[15] Rwanda and Uzbekistan are not outliers. 78 percent of the world's internet users live in countries where simply expressing political, social, and

---

[12] *E.g.*, 50 U.S.C. § 1702(b)(3) (restricting Presidential authority to regulate importation of "any information or informational materials"); *In re Amendment of Section 64.702 of the Commission's Rules and Regulations*, 77 F.C.C.2d 384, 429, para. 116 (1980) (Second Computer Inquiry) (ensuring "nondiscriminatory access to common carrier telecommunications facilities" by providers of information services).
[13] *Transparency Reports*, Wikimedia Foundation, here (last visited Feb. 13, 2024).
[14] *Rwanda*, Freedom House (2023), here.
[15] Catherine Putz, *Uzbekistan Unblocks Twitter, TikTok Still Restricted*, The Diplomat (Aug. 4, 2022), here.

religious viewpoints leads to legal repercussions.[16] The United States should maintain its longstanding opposition to these requirements.

While there are a range of reasons companies have resisted data localization requirements, some are at least in part doing so over concerns they will be complicit in government repression. When data is not stored locally, the respective government often must go through a legitimate – albeit far from perfect[17] – legal process for accessing the information from U.S. companies. But when data is stored on local servers, the ability for companies to resist problematic state demands is hampered. This challenge is further compounded by the emergence of so-called hostage-taking laws, in which international companies are required to have a local presence in a particular country, curbing their willingness to push back against user data requests over concerns for employee safety.

Nonetheless, firm commitment to a free and open internet does not mean surrender to an *unregulated* internet. For example, U.S. civil rights statutes apply to foreign entities that discriminate against individuals in the United States,[18] and neither housing data abroad nor engaging in international data flows will undermine domestic regulation of discriminatory algorithmic decision-making. Regulations of data and AI such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act became law years ago, and there has been no credible challenge under international trade law to either, despite pro-business commentary insisting as much.

Moreover, well-scoped exceptions in treaty language can help protect regulatory goals in regulation of data and AI. International digital trade agreements have long sought to accommodate legitimate public policy objectives. For example, the USMCA recognized an exception to its prohibition on restricting cross-border data flows to "achieve a legitimate public policy objective."[19] Well-scoped exceptions in negotiations at the WTO and elsewhere may similarly allow for flexibility for domestic regulation to address emerging harms; indeed, some of the signatories of this letter have recognized the need to ensure that international agreements do not "thwart" algorithmic impact assessments and audits.[20]

---

[16] Allie Funk et al., Freedom on the Net 2023 (2023), here.
[17] Access Now, ACLU, CDT, et al., Coalition letter on CLOUD Act (Mar. 12, 2018), here.
[18] Equal Employment Opportunity Commission, Enforcement Guidance on Application of Title VII and the Americans with Disabilities Act to Conduct Overseas and to Foreign Employers Discriminating in the United States (1993), here ("By employing individuals within the United States, a foreign employer invokes the benefits and protections of U.S. law. As a result, the employer should reasonably anticipate being subjected to the Title VII enforcement . . . . ").
[19] Agreement Between the United States of America, the United Mexican States, and Canada, July 1, 2020, art. 19.11, here.
[20] Letter form Lawyers' Committee for Civil Rights, ACLU, CDT et al. to President Joseph R. Biden at 2 (May 23, 2023), here.

Similarly, Congressional leaders have recognized that source code protections should "ensure that countries [cannot] force businesses to surrender their source code or share it with domestic competitors as a condition of doing business, while preserving the ability of governments to access source code to achieve legitimate public policy objectives, such as conducting investigations and examinations and promoting consumer health and safety."[21] Long-standing U.S. policy supporting an open internet is fully consistent with exceptions to achieve these legitimate public policy objectives.

But these exceptions should be concrete and appropriately scoped. The United States should lead *both* in establishing thoughtful regulations to support equity and privacy *and* in protecting an open and free internet. The United States should clarify immediately that both sets of goals remain at the heart of U.S. policy.

We thank you for your consideration. Please do not hesitate to contact us at cvenzke@aclu.org.

Sincerely,

American Civil Liberties Union
Center for Democracy & Technology
Freedom House
Information Technology and Innovation Foundation
Internet Society
PEN America
Wikimedia Foundation

Signatories in their individual capacities:
Susan Aaronson, Ph.D., Director, Digital Trade and Data Governance Hub, George Washington University and co-PI NIST-NSF Trustworthy AI Institute at George Washington University
Fiona Alexander, Senior Fellow, Digital Innovation Initiative, Center for European Policy Analysis (CEPA)
Dr. Konstantinos Komaitis, Internet Governance expert
Professor Peter Swire, J.Z. Liang Chair, School of Cybersecurity & Privacy, Professor of Law and Ethics, Scheller College of Business at Georgia Institute of Technology

cc: Neema Singh Guliani
Shannon Coe
Brian Daigle

[21] Congressional Letter at 2-3.

Valerie Santos
Robert Tanner
Jillian DeLuna
Tarun Chhabra
Christina Segal-Knowles