Fiona Alexander, Associate Administrator
Office of International Affairs
National Telecommunications & Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4701
Washington, DC 20230
(via email at iipp2018@ntia.doc.gov)

July 06, 2018

Re: Notice of Inquiry on International Internet Policy Priorities (Docket No. 180124068-8068-01)

Ms. Alexander,

Thank you for this opportunity to provide feedback to the National Telecommunications & Information Administration's (NTIA) international internet policy priorities, which requests guidance to "help NTIA and the U.S. Government identify the most important issues facing the internet globally." NTIA's Office of International Affairs structured the notice of inquiry by asking a series of questions in four broad categories: (1) The free flow of information and jurisdiction; (2) the multistakeholder approach to internet governance; (3) privacy and security; and (4) emerging technologies and trends.

About Access Now:

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally, we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those most at risk. We serve on the European Commission Expert Group on the application of the General Data Protection Regulation, we are accredited with the United Nations Economic and Social Council, and we host RightsCon, the world's leading conference on human rights in the digital age.

The Free Flow of Information and Jurisdiction

A. What are the challenges to the free flow of information online?

1. **A growing number of laws being proposed that would limit free expression and restrict online privacy**. This includes laws to limit encryption, regulate content, and alleged "cybersecurity" or "cybercrime" laws that go far beyond justifiable scope. Such laws are often advanced under the banner of protecting national security, yet they have far-reaching

negative implications for the free flow of information online, and upon review, fail to hide the real intent.

2. **An increase in internet shutdowns and network restrictions that harms free expression and drains billions from the global economy.** In 2017, there were more than 100 internet shutdowns, and in 2018 there have already been 81. The number of shutdowns is dramatically increasing, and some countries are repeat offenders. Governments frequently justify shutdowns on the pretext of increasing public safety, stopping the spread of disinformation or illegal content, preventing cheating on school exams, or on vague grounds of national security. Access Now has found that shutdowns take place during protests, during periods of political instability, and surrounding elections.[1]

3. **An increase in cyber attacks against news outlets and activists.** Along with the rise in large-scale cyber attacks that have caused significant data breaches and disruption to the internet, over the past five years Access Now's Digital Security Helpline has witnessed a 20-fold increase in targeted attacks on news outlets, activists, and political opposition groups. This includes Distributed Denial of Service (DDoS) attacks, which render websites effectively inaccessible, including during elections, periods of political unrest, or when there is publication of content that a government wants to repress. It also includes hacking of devices or accounts, often involving large-scale phishing campaigns and coordination across countries. Such attacks are increasingly cheap and simple to conduct, and have been further enabled through the proliferation of corporate hacking products. Activists and media outlets often have few defenses against such attacks, and are under-resourced and underprepared.[2]

4. **Restrictions on access to VPNs and other circumvention tools that enable people to securely connect to the global internet.** Circumvention tools are vital in countries that censor the internet. Unfortunately, authoritarian governments consistently seek to shut them down to prevent people from gaining unfettered access to the internet. Fourteen countries now restrict VPNs in some form, with six having introduced restrictions in the past year.[3] Access to circumvention tools suffered another blow recently when Google and Amazon disabled a technique known as "domain fronting," which works by routing internet through the infrastructure of the tech companies in order to obscure the actual destination of the traffic. Domain fronting enables hundreds of millions of people in authoritarian countries to evade state censorship. It prevents governments and state-controlled internet service providers from shutting down circumvention tools without paying the heavy price of blocking access to the whole suite of Amazon or Google products.

[1] See https://www.accessnow.org/keepiton/

[2] See https://freedomhouse.org/report/freedom-net/freedom-net-2017, https://www.derechosdigitales.org/wp-content/uploads/HT-map.png, https://motherboard.vice.com/en_us/article/wnxpjm/nso-group-new-big-player-in-government-spyware and https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

[3] https://freedomhouse.org/report/freedom-net/freedom-net-2017

More than a dozen U.S. government-funded tools have been made available through domain fronting, including Tor, Psiphon, Ultrasurf, Signal, Greatfire, and Lantern. These tools allow millions of people to access the free and open internet and communicate securely. Major public and private international media companies, including *The New York Times* and the *Associated Press,* rely upon these tools to reach audiences within repressive countries who otherwise would not have access to a free press. With this decision, Google and Amazon have capitulated to authoritarian governments, and ultimately aided these regimes' efforts to limit access to information, at a dire cost to democracy and the human rights movements in these countries.[4]

B. Which foreign laws and policies restrict the free flow of information online? What is the impact on U.S. companies and users in general?

1. **Limits on encryption.** Encryption is fundamental to the security of the internet, from defending connected critical infrastructure to protecting people from criminal activity online. It is also the cornerstone of today's digital economy, and its use has powered the ability to trust and authenticate interactions and communicate and conduct business safely across borders in the digital age. However, law enforcement and intelligence agencies around the world, including the Australia, India, Brazil, and the United Kingdom, have called on companies to provide special access (a.k.a. "backdoors") to encrypted communications and/or devices for use in investigations.[5]

   Undermining encryption via backdoors hurts the security of the internet overall. To date, every proposal for a mechanism to allow law enforcement to bypass encryption has been found to have security flaws that could cause grave harm to people, governments, and infrastructure. Furthermore, undermining encryption will not solve law enforcement's problems. An "encryption backdoor just for the good guys" would be impossible to implement, as it would open the door to abuse by less scrupulous governments and would simply push criminals and terrorists onto alternative encrypted services that are difficult to regulate.[6]

   Finally, many countries have limited the import and export of encryption software.[7] This

[4] *See* https://www.accessnow.org/cms/assets/uploads/2018/05/5.7.18-Letter-to-Congress-_-Domain-Fronting.pdf

[5] *See* https://securetheinternet.org/

[6] *See* https://www.justsecurity.org/53316/criminalize-security-criminals-secure/, https://www.accessnow.org/testimony-before-the-parliament-of-australia-parliamentary-joint-committee-on-law-enforcement/ and https://www.accessnow.org/cms/assets/uploads/2018/02/Encryption-in-the-United-States-Crypto-Colloquium-Outcomes-Report.pdf

[7] *See* https://www.gp-digital.org/world-map-of-encryption/ for an interactive map of encryption limitations around the world.

not only causes barriers to cross-border information flow, but also endangers activists, journalists, lawyers, and others who rely on the the protection of encryption. Indeed, the United Nations Special Rapporteur for Freedom of Expression has stated, “encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.”[8]

2. **Repressive cybersecurity and cybercrime laws.** As cybersecurity threats and cybercrime continue to grow around the world, authoritarian governments in countries such as Vietnam and Egypt have passed laws that go far beyond any legitimate scope, restricting free expression, infringing upon online privacy, and empowering state surveillance under the pretense of national security.[9]

3. **Data localization laws.** With renewed energy since the revelations of government surveillance made possible by Edward Snowden, governments around the world have pursued forced data localization — requiring tech companies to store data in-country. Lawmakers typically argue that such measures ensure data security and boost the local IT sector via infrastructure investment. However, these laws actually undermine data security by allowing governments increased control over online activities, enabling surveillance and risking the rights to privacy and free expression. They also force companies to forego legal protections granted to users under other jurisdictions. For example, Vietnam’s cybercrime law, referenced above, includes a data localization provision that requires companies to have a local office and store data of Vietnamese users within the country.[10]

   Data localization requirements also harm economic development by imposing significant financial costs on companies, who must build local data centers and alter their technical infrastructure. Currently, most companies keep multiple copies of user data across multiple data centers to efficiently balance storage and deliver content. Forcing traffic to go through specific countries slows speeds and leads to fragmentation of the internet. Data localization also impedes innovation. Small and medium-sized companies are unlikely to have the resources to adapt to such significant regulatory changes, and the high financial costs of implementing data localization increases barriers to entry for start-ups.[11]

[8] *See* https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[9] *See* https://www.washingtonpost.com/world/asia_pacific/vietnam-passes-cybersecurity-law-despite-privacy-concerns/2018/06/12/f4b27ce2-6dfb-11e8-b4d8-eaf78d4c544c_story.html?utm_term=.98f47616e308 and https://www.madamasr.com/en/2018/06/05/news/u/parliament-passes-cybercrime-law-regulating-web-content-and-isp-surveillance/

[10] https://techcrunch.com/2018/06/12/vietnams-new-cyber-security-law-draws-concern-for-restricting-free-speech/

[11] *See* https://www.accessnow.org/the-impact-of-forced-data-localisation-on-fundamental-rights/

4. **Lack of data protection laws.** Although data protection laws are slowly becoming more common around the world, they are not yet in place everywhere. This has resulted in jurisdictional clashes between countries with data protection requirements and those without. Notable examples are the European Union's General Data Protection Regulation (GDPR) and the Privacy Shield arrangement between the EU and the United States. Currently, Privacy Shield is in violation of the standards outlined by the GDPR: it fails to provide effective individual redress mechanisms or independent oversight. Such discrepancies will no doubt result in legal challenges and disrupt information flows.[12]

C. Have courts in other countries issued Internet-related judgments that apply national laws to the global Internet? What have been the practical effects on U.S. companies of such judgements? What have the effects been on users?

The 2016 Investigatory Powers Act granted the UK government sweeping mass surveillance powers, including extraterritorially, by, among other things, greenlighting state hacking of devices, networks, and services on foreign soil.[13] The law, which remains in effect, has been declared unlawful by the UK's Court of Appeal.[14] The CLOUD (Clarifying Lawful Overseas Use of Data) Act was passed by the U.S. Congress in March 2018. The CLOUD Act enables the U.S. to get direct access to data stored abroad, and allows the U.S. to enter into agreements with other countries so they can directly order data from companies in the U.S. Should the U.S. and UK reach an agreement under the CLOUD Act, the UK would be able to apply the IP Act within the U.S. subject primarily to the narrow safeguards in British law [15]

D. What are the challenges to freedom of expression online?

1. **Pressure on tech companies to regulate online content.** Social media platforms have been used to disseminate and spread misinformation, so-called "fake news," and terrorist propaganda. Today, people from marginalized groups continue to face harassment on social media, and violent hate groups have used these platforms to organize mass gatherings. This has led government officials around the world to push companies like Facebook, Twitter, and Google to "take action." Legislative proposals to restrict speech in some form have arisen in Brazil, Nicaragua, Mexico, Honduras, Malaysia, Uganda, Tanzania, and even the U.S., among others. Unfortunately, by focusing on ways to block or filter out the "bad" content, these proposals have significant implications for free expression and the future of the open internet.

[12] *See* https://www.accessnow.org/access-now-urges-european-commission-push-us-surveillance-reform-privacy-shield-review/

[13] *See* https://techcrunch.com/2016/11/29/yes-the-uk-now-has-a-law-to-log-web-users-browsing-behavior-hack-devices-and-limit-encryption/

[14] https://www.theverge.com/2018/1/30/16949520/uk-mass-surveillance-illegal-dripa-court-of-appeal

[15] *See* https://www.accessnow.org/what-happened-with-the-cloud-act-and-what-comes-next/

At their most extreme, government proposals seek to force companies to monitor, interpret, police, and sometimes block user content. These are all acts of censorship, and can interfere with the right to free expression. Although this right is considered internationally to be a "qualified" right, meaning it can be limited when absolutely necessary to serve a legitimate government interest, repressive governments often abuse this qualification and restrict important, legitimate speech that ultimately restricts research, discourages dissent, and silences unpopular ideas.[16]

Many government proposals also seek to require or coerce privatized enforcement of speech laws, delegating the role of censor to private companies without adequate judicial oversight or public accountability. This is dangerous, since private companies are not held to the same human rights standards as governments, and without proper human rights protections, any authority delegated to them is likely to be exercised over-broadly. This could lead to the removal of lawful content on a mass scale, as companies are likely to avoid legal liability by reducing risk. This tendency has already been documented. For example, companies often remove legitimate content because they face false claims under intellectual property law.[17]

2. **Increased demands to register with legal identities to gain access to networks.** Digital identity is increasingly the focus of policy discussions across several different countries, including Australia, Estonia, Tunisia, Nigeria, and India, with a number of governments proposing or implementing national digital identity programs, and multilateral institutions making investments. Through these government-administered or coordinated programs, governments often aim to provide a single digital identity to residents. Many such programs entail a push to collect, store, and use the biometrics of individuals as the primary means of establishing and authenticating their identity.

   Proponents of centralized national ID programs, particularly those promoting biometric linkage, argue that they bring benefits such as more accurate and efficient delivery of government services; that they can reduce corruption or increase inclusion; or can help serve national security interests. Critics have responded by noting that national digital identity schemes may not in fact ensure more effective distribution of benefits, better service delivery, or improved governance, and at the same time, the programs are designed or governed poorly; catalyze social exclusion; fail to protect the rights to privacy and data protection; and create new cybersecurity threats.

   Any initiative to legally mandate a centralized national digital identity program poses significant risks for human rights. Specifically, they threaten to undermine the right to privacy and chill the freedom of movement and freedom of expression. Further, since digital identify programs typically entail the creation of centralized troves of sensitive

[16] *See* https://www.accessnow.org/brazil-fake-news-proposals-add-uncertainty-to-institutional-crisis/ and https://www.accessnow.org/fisherman-soccer-cattle-malaysia-tanzania-censorship/
[17] *See* https://www.accessnow.org/saving-agnostic-internet-part/

personal data, susceptible to breach by malicious actors or abuse by public authorities, they also carry the potential to turn a digital ID into a pervasive means of identification, tracking, or control, especially when such identities are biometrically linked and made mandatory. To address this, it is imperative that the safeguards -- legal, technological, and procedural -- be adopted holistically.[18]

F. What role can NTIA play in helping to reduce restrictions on the free flow of information over the Internet and ensuring free expression online?

NTIA has an effective voice both through international forums and through norm-setting and thought leadership in the U.S. government. Access Now recommends NTIA use its resources and authority to:

- Promote digital security through support for strong encryption and the inclusion of human rights principles in cybersecurity laws and policies, and opposing public or private censorship regimes;
- Oppose internet shutdowns globally and support greater transparency around policies, including U.S. policies, that allow or require networks or services to be disabled;
- Support rights-based cybersecurity processes, including by:
    - Opposing restrictions on circumvention tools and providing educational resources on the impact of cyberattacks, including the impact on end users;
    - Promoting security research as well as the disclosure of vulnerabilities to entities best positioned to create and issue patches for products and services;
    - Educating on the role and value of threat intelligence sharing with high-risk populations; and
    - Supporting the right to your own infrastructure and community-level networking devices and services, as through municipal networks, mesh, and alternative telecommunications networks;
- Support the free and open internet by working with stakeholders to draft model data protection laws, including for implementation within the U.S., opposing all data localization mandates internationally, and actively lobbying for strong human rights protections for any international agreements that would expand government access to user data;
- Protect free expression internationally, including by issuing guidance to companies regarding best practices for removing content that is not subject to a legal order and analyzing best practices for reporting (and responding to reports) of abuse and harassment online; and
- Promote the need for human rights protections in domestic or international digital identity regimes.

[18] *See* Access Now policy paper on national digital identity programs: https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

Multistakeholder Approach to Internet Governance

A. Does the multistakeholder approach continue to support an environment for the Internet to grow and thrive? If so, why? If not, why not?

The multistakeholder approach of internet governance is vital for the future of an open global internet. Particularly important has been the inclusion of civil society voices in the internet governance debate. The perspectives represented by civil society are not only informative for the technological, business, and government participants, they also serve as the voice of the people, especially in countries that restrict human rights and prevent independent voices from participating.

B. Are there public policy areas in which the multistakeholder approach works best? If yes, what are those areas and why? Are there areas in which the multistakeholder approach does not work effectively? If there are, what are those areas and why?

The development of cybersecurity policy benefits from multistakeholderism. Unfortunately, cybersecurity forums continue to be dominated by militarist, foreign policy, or corporate interest-focused discourses in which civil society views and the importance of protecting human rights are ignored.

Cybersecurity policy and norm establishment should involve effective participation of all stakeholders. This sort of open process should be supported by a pluralistic inclusion of stakeholders whereby various actors and groups are given equitable access and are proactively approached for input and participation with a realistic timeframe.[19] The policymaking process must also be transparent throughout its duration, with clear lines of communication and feedback with all parties, and include a mechanism for appeal and challenge.

D. Should the IANA Stewardship Transition be unwound? If yes, why and how? If not, why not?

Access Now supported the transition of IANA functions to the multistakeholder community. Supporting the participation of a diverse international multistakeholder community is the most robust long-term strategy for preventing any governments or other entities from steering the Domain Name System (DNS) in a direction that would be much less supportive of a free and open global internet. Further, the IANA transition provided an effective path to continued stable and resilient DNS administration that supports the interests of public and private stakeholders across societies and industries.

[19] *See* https://www.accessnow.org/cms/assets/uploads/2017/11/A-Policy-Makers-Guide-to-GCCS-2017-digital-v.pdf

The transition of these functions away from the U.S. government removed an excuse for authoritarian countries to demand greater oversight and regulation of internet issues. The open, interoperable, global internet did not arise out of agreements between governments, but rather through community-led innovative approaches by diverse stakeholders. In many ways, this transition returned the internet and DNS to the open multistakeholder governance model that characterized and fostered its first few decades of growth.[20]

G. Are there barriers to engagement at the IGF? If so, how can we lower these barriers?

The acceptance of the multistakeholder model has resulted in much greater participation of civil society at the IGF and its regional subsidiaries. Nevertheless, a number of barriers remain. First, there needs to be greater support for civil society from government stakeholders. This includes funding for civil society participants to attend the IGF. Many local and regional organizations lack the financial resources to attend, yet their voices and experience are vital to the conversations taking place.

There also needs to be greater inclusion of civil society into discussions about and around the IGF. The regionalization of the IGF and inter-sessional work have provided important avenues for civil society engagement on specific issues relevant to their particular contexts. This approach should continue, and the bodies governing the regional events and inter-sessional programs should endeavor to further integrate civil society into both the planning and implementation of IGF-related events.

Privacy and Security

B. Which international venues are the most appropriate to address questions of digital privacy? What privacy issues should NTIA prioritize in those international venues?

Access Now recommends greater engagement at user-focused conferences and events. One place where NTIA representatives could engage is RightsCon, the world's leading conference on human rights in the digital age. RightsCon brings together business leaders, policymakers, general counsels, government representatives, technologists, and human rights defenders to tackle pressing issues at the intersection of human rights and digital technology.

RightsCon is where the global community comes together to break down silos, forge partnerships, and drive large-scale, real-world change toward a more free, open, and connected world.[21] At RightsCon, NTIA would be able to engage with activists and members of the global digital rights community to learn more about privacy issues faced by different actors around the world.

[20] *See* https://www.accessnow.org/cms/assets/uploads/2016/05/CSstatementonIANAtransitionMay2016-1.pdf

[21] https://www.rightscon.org/

Emerging Technologies and Trends

A. What emerging technologies and trends should be the focus of international policy discussions? Please provide specific examples.

1. **Artificial Intelligence and machine learning.** Advances in Artificial Intelligence (AI), particularly machine learning, hold promise for helping solve some of the world's greatest problems. Already, deep learning techniques have enabled the creation of AI that can diagnose disease more accurately and drive cars more safely than humans.

   However, a growing number of cases in the U.S. show that outputs are often far from neutral, and can have direct, negative impacts on people's lives. This happens in cases where AI systems are used to make decisions about people, including in the assignment of credit scores, identification of job candidates, or ranking students for college admissions. Because they rely on mathematics rather than human decision-making, these systems are often seen as objective and the outputs they produce are rarely questioned. Unfortunately, they are often also implemented with little care to issues of bias and data quality that are inherent to all algorithmic decision-making methods.

   Given the rapid pace of development and use of AI, law and policy must catch up. To this end, Access Now and Amnesty International recently launched the Toronto Declaration, which states that the risks for discrimination posed by machine learning systems must urgently be examined and addressed at the governmental level and by the private sector conceiving, developing, and deploying these systems. Companies and civil society organizations, including those who engage with the NTIA, can demonstrate their commitment to protecting users against these risks by endorsing the Toronto Declaration.[22]

2. **Security, privacy, and the Internet of Things.** The dangers of insecure IoT devices have already been demonstrated by the series of massive IoT-enabled DDoS attacks that took down large swaths of the internet.[23] Unfortunately, little is being done to prevent such events from occurring in the future, and the companies that produce IoT devices actively resist adhering to robust security standards. As technology becomes more embedded in our lives via the development of wearables and implanted tech, we are increasingly vulnerable to manipulation and exploitation. As we move further toward this integration of technology and ourselves, we must develop adequate data protection and surveillance laws that protect individuals from misuse, manipulation, and weaponization of their data and devices.

[22] *See* the Toronto Declaration here: https://www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf
[23] http://www.wired.co.uk/article/minecraft-mirai-botnet-ddos

Conclusion

We appreciate the NTIA's engagement with the international community and trust this feedback will assist the agency in determining the most important issues facing the global internet. NTIA's Office of International Affairs has a valuable role to play in addressing these issues within the international community. We look forward to continuing to work with your office to promote a free and open internet that respects the human rights of all users.

Thank you,

Amie Stepanovich
U.S. Policy Manager
Access Now

Nathan White
Senior Legislative
Manager
Access Now

Lindsey Andersen
Policy Intern
Access Now