Fiona Alexander, Associate Administrator
National Telecommunications and Information Administration,
U.S. Department of Commerce
1401 Constitution Avenue, NW, Room 4725
Washington, DC 20230
iipp2018@ntia.doc.gov

July 17, 2018

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

Comments by the Global Digital Protectionism Project

Dear Ms. Alexander:

Thank you for this opportunity to comment on international internet policy priorities.

About us:

The Global Digital Protectionism Project examines how officials, business, and civil society around the world define barriers to cross-border data flows and provides insights as to whether there are shared norms and strategies to address digital protectionism. The project is funded by the Hewlett Foundation and other think tanks, and is staffed in the US and the EU. The project examines the US, EU, Canada, Brazil and Russian internet markets and we also have a survey available to respondents globally at

https://goo.gl/forms/DRAEBWRY942wP6tE2

Our response will address: I. The free flow of information and jurisdiction II. Multistakeholder approach to internet governance III. Privacy and Security; and IV. Emerging Technologies and Trends.

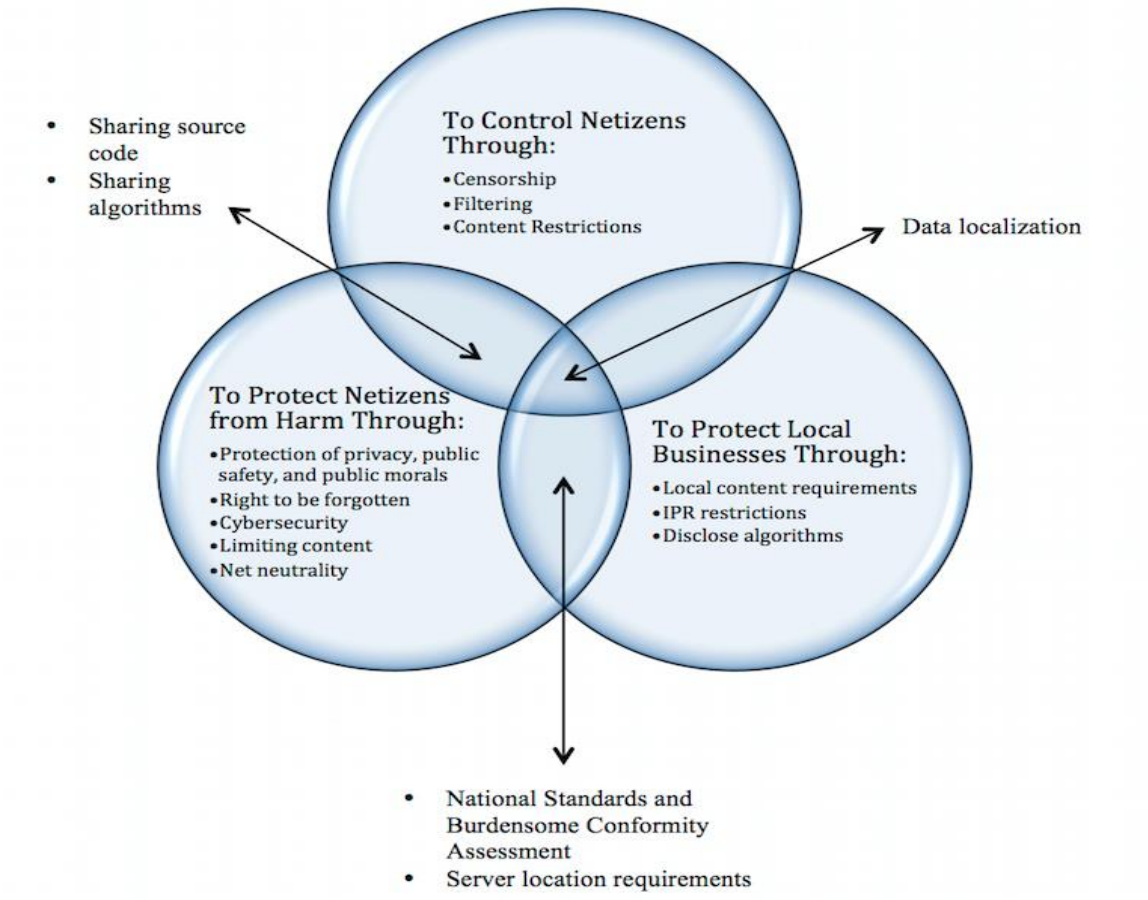
Please note that herein we use data and information interchangeably but we recognize that they are not the same. Information is processed data.

I. The Free Flow of Information and Jurisdiction

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

The free flow of information/data across borders is regulated by trade agreements that govern e-commerce and digital services. UNCTAD and the World Bank have collaborated with a wide range of governments to establish domestic yet interoperable rules on e-signatures, spam, cybersecurity etc. But while there is a consensus on the rules to govern e-commerce, there is no consensus internationally as what is legitimate domestic regulation for the data driven economy (AI, apps, data analytics, IoT etc.…) and what is trade distorting. As a result, governments can justify practices such as censorship, internet shutdowns, filtering, cyber-security, etc. under the exceptions contained in trade agreements. Exceptions allow nations to breach the rules to achieve domestic policy goals, but trade agreement participants can still be subject to trade disputes.

Figure 1: Why and How Do Governments Restrict Cross-Border Information Flows?



Source: Aaronson, World Trade Review

Censorship provides a good example. The US government routinely condemns censorship as a barrier to trade, although it has never challenged such behaviour in a trade dispute. However, in

2016, the United States cited China's Great Firewall as a trade barrier, which could mean that the United States is gathering evidence to challenge broad censorship (USTR 2016b). In 2018, the United States asked the WTO services council to discuss China's cybersecurity rules as a barrier to the free flow of data (WTO 2018)[1]

The EU also criticizes censorship (including the Great Firewall) as a barrier to trade. Yet the EU provides its citizens with a right to request delinking of sites—the 'right to be forgotten'. If an individual asks to be forgotten and an ISP approves the request, the information will remain online at the original site but will no longer appear under certain search engine queries. Some ISPs may interpret such requests as onerous and trade-distorting, while some human rights activists believe that delinking undermines the public's access to information.

Other governments censor indirectly. Governments increasingly require internet firms to take down site content internet-wide that may be breach local intellectual property rules. Some observers consider such takedown requirements a form of censorship that can distort trade, especially when a government's court requires that the decision be enforced internet-wide, as occurred in a Canadian court case. In June 2017, in *Google Inc. v. Equustek* Solutions Inc., 2017 SCC 34, a majority of the Supreme Court of Canada upheld a worldwide interlocutory injunction that required Google to globally de-index the webpages of a defendant in a separate intellectual property infringement proceeding.[2] In 2016, French Data Protection Authority (CNIL) declared that search engines implementing France's Right to Be Forgotten law must de-list such links globally and not simply take down such sites within the EU . On July 19, 2017, France's highest administrative court, the Conseil d'Etat (in English, the Council of State) referred the dispute between CNIL and Google over the legality of applying the right to be de-indexed globally to the Court of Justice of the European Union (CJEU). A Paris-based NGO, Internet and Jurisdiction, closely monitors such cases noting that the number and impact of such cases increasingly distort cross-border data flows (Internet and Jurisdiction 2017). If other countries mandate similar decisions regarding site takedowns, firms such as Google would struggle to comply with potentially conflicting laws and these national decisions could yield international jurisdictional conflicts.

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?

The US Trade Representative annually prepares a list of barriers to digital trade and not to the free flow of information. It includes: data localization requirements, filtering and blocking laws, intellectual property laws, intermediary liability laws, requirements to divulge source code, and national standards and conformity assessments. The US is the only country that fully defines and

[1] Susan Ariel Aaronson, "What are What Are We Talking about When We Talk about Digital Protectionism? "World Trade Review, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032108

[2] Supreme Court of Canada, *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34 (2017).

reports annually on these barriers.[3] However, the US has done little to build consensus on what are these barriers and to educate policymakers in other countries as to the economic costs of these barriers. (In this regard, the US seems to rely on the OECD.)

Among the most important barriers is the use of national security or cyber-security rationales to justify local server requirements, disclosure of source code or algorithms, or censorship.

H. How might NTIA better assist with jurisdictional challenges on the internet?

The NTIA should work with other agencies such as USTR, DOS, and DOT, to ensure that there is a coherent approach to governing cross-border flows.

a. On the free flow of information. It will not be easy to set international rules to limit restrictions on the free flow of information without a shared set of norms and definitions. The NTIA should utilize the multistakeholder process to help set norms and better define when national policies unfairly distort the free flow of information. While doing this, the NTIA should think of the internet more holistically bringing together a more comprehensive set of stakeholders.

b. On policy coordination The US needs an internet coordinator to work with the many diverse agencies on cross-cutting internet governance issues. A senior official at NTIA could fulfill this function.

II. The Multistakeholder approach to internet governance

NTIA should continue to rely on multistakeholder venues such as IGF, ICANN, IETF and others such as the Internet and Jurisdiction Policy network. While often it's the same people who attend these meetings, it is increasingly younger people who get that they are responsible for internet governance. These meetings provide a town hall for the internet, and as in a town hall, only some people are motivated to speak out consistently. NTIA could fund internships and student coursework as internet governance should be an element of civic education.

Should the IANA Stewardship Transition be unwound?
No.

III. Privacy and Security

Privacy and security are essential components of a trusted internet. NTIA should develop efforts to transition to a data driven economy built on the ability of people to control their data. Thanks to the mobile internet, the internet of things and other data driven technologies. almost all our daily activities are data collection opportunities (NIST: 2018). In the past,

[3] https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital

researchers had to obtain (or at least go through the motions of) obtaining consent. However, with the data driven economy, people whose data is collected and used have provided their personal data without fully informed consent. (People don't understand that in return for providing data that firms then monetize, they receive the many free services presented by digital technologies.[4] But people do understand that they have lost control over data that belongs to them. Recent survey data shows that people around the world are increasingly concerned about how firms use, protect, control, and trade personal data. For example, the US Government found that Americans are increasingly concerned about online security and privacy after recent data breaches, cybersecurity incidents, and controversies over the privacy of online services[5] A 2016 Eurobarometer survey found that some 90% of respondents say it is important that personal information pictures, contact lists, etc.) on their computer, smartphone or tablet can only be accessed with their permission. Some 82% of those polled also say it is important that tools for monitoring their activities online (such as cookies) can only be used with their permission.[6] A 2018 poll of 25,262 internet users in 25 countries found that half of internet users surveyed around the world are more concerned about their online privacy than they were a year ago, reflecting growing concern around the world about online privacy and the power of social media platforms. [7]

Other governments are starting to provide greater control over data to their citizens as example Europe and Brazil. Citizens in Colombia and Mexico have constitutional rights to control over their data.[8] However, many developing countries don't yet have effective rules protecting personal data online. These countries don't have data sectors although most have growing numbers of people online. Many developing countries have not viewed privacy regulation as essential to equitable and efficient economic growth. UNCTAD did a 2015 survey of its 194 members, UNCTAD found that some 58 percent of its member states had only privacy laws to facilitate an effective enabling environment.[9] NTIA should work with these governments to help them improve their enabling environment.

---

[4] Australian Government Productivity Commission, 2017. Data Availability and Use, Productivity Commission Inquiry Report: Overview and Recommendations, No. 82, 31 March.

[5] Goldberg, Rafi, 2016. Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NTIA, Department of Commerce, https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

[6] Eurobarometer, 2016. Briefing Note, December, http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124`

[7] CIGI, 2018, 2018 CIGI-Ipsos Global Survey on Internet Security and Trust, https://www.cigionline.org/internet-survey-2018

[8] For a good overview see DLA Piper, Data protection laws of the world," https://www.dlapiperdataprotection.com/

[9] UNCTAD. 2015. Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned, TD/B/C. II/EM.5/2. January 14. http://unctad.org/meetings/en/SessionalDocuments/ciiem5d2_en.pdf

For the data driven economy to succeed, the providers of personal information must have the rights to control their data. Policymakers should call for an international meeting to establish an interoperable approach to data protection and control which allows nations to evolve their own complementary approaches. The meeting should be attended by a diverse group of individuals, firms and agencies involved in privacy and data protection issues, and it should be tasked to build on existing principles such as the APEC and OECD Privacy Principles. [10]

IV. Emerging Technologies and trends

What emerging technologies and trends should be the focus of international policy discussions?

NTIA should engage in a discussion with likeminded governments about the international policy implications of AI. While many countries have firms with AI expertise (e.g. Germany in autonomous cars, Canada in machine learning), many countries have no expertise whatsoever. Developing countries are likely to have the most problems adapting to the data driven economy. These countries will be customers of AI and other data driven sectors, rather than producers of AI. According to Kai-Fu Lee, a venture capitalist and former computer scientist, the bulk of profit from the data-driven economy and particularly artificial intelligence will go to the United States and China. "A.I. is an industry in which strength begets strength: The more data you have, the better your product; the better your product, the more data you can collect; the more data you can collect, the more talent you can attract; the more talent you can attract, the better your product. It's a virtuous circle, and the United States and China have already amassed the talent, market share and data to set it in motion." He also notes these countries will have growing populations with little future of jobs without more years of education. Without those workers earning adequate income, states won't be able to raise sufficient revenue to help their workers gain sufficient education.[11]

A growing number of governments including the UK, China, and France, have developed national plans for AI. These governments have already started to see machine learning as the core differentiating technology of the twenty first century. We agree with Ian Hogarth, who says that machine learning could become a huge differentiator between states--economically, militarily and technologically. It could trigger an AI arms race.[12] This competition to achieve leadership on AI will have important spillovers for foreign policy, governance, taxation, peace etc.…It could also create significant political and social instability. The US should be leading this discussion, but the US may have less credibility given its current protectionism and the decision by the Trump

[10] On APEC principles, see https://www.apec.org/-/media/APEC/.../APEC-Privacy.../05_ecsg_privacyframewk.pdf; and OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[11] Kai Fu Lee, "The Real Threat of Artificial Intelligence,' NY Times, June 24, 2017, https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html

[12] Ian Hogarth, AI Nationalism, https://www.ianhogarth.com/blog/2018/6/13/ai-nationalism

Administration to abandon the one trade agreement with binding data flow provisions that govern AI.

NTIA could play a useful role here by encouraging other nations to make algorithms a public good as with TCP/IP or GPS. . The US could build on the work of Open AI, a non-profit AI research company, which aims to ensure that AI is developed in an ethical manner that is good for humanity.[13] In addition, the US should encourage global norms regarding ethical regulation of AI.[14]

Conclusion

Thank you for this opportunity to assist NTIA in its important work with the global community on internet issues.

Susan Ariel Aaronson, Ph.D.
Research Professor of International Affairs and Cross-Disciplinary Fellow, GWU
Senior Fellow, Centre for International Governance Innovation
Director, Global Digital Protectionism Project

Thomas Struett
Survey Director and Senior Analyst

[13] https://openai.com/
[14] http://cyber.harvard.edu/topics/ethics-and-governance-ai