NISKANEN CENTER

Regulatory Comment

Comments submitted to the National Telecommunications and Information Administration in the Matter of:

INTERNATIONAL INTERNET POLICY PRIORITIES

Ryan Hagemann
Senior Director for Policy
Niskanen Center

Alec Stapp
Technology Policy Fellow
Niskanen Center

Submitted: July 17, 2018
Docket Number: 180124068-8068-01

EXECUTIVE SUMMARY

One of the primary challenges to the continued free flow of information and speech online is the potential for a "control-driven model" of global Internet governance to supplant the existing American-inspired order. National laws and regulations, promulgated by countries around the world, could potentially impede cross-border information flows, to the significant detriment of not only U.S. companies and private sector interests, but free expression and human rights as well. But the threats to the current paradigm of multistakeholder-driven Internet governance do not spring only from nation-states. The emergence of advanced technologies, such as automated botnets, hold the potential to devolve considerable power over the globally-networked digital ecosystem into the hands of non-state actors. It is a fragile time for the Internet.

To combat these many emerging threats, it is imperative that the United States continue to play a leading role in defending the existing order for Internet governance. Digital commerce and trade requires a consistent, predictable, and simple legal environment to maximize the benefits to human beings worldwide. The right to freedom of expression, similarly, requires certainty and trust in an online environment made possible by a consensus-driven model of governance, led by stakeholders from industry and civil society capable of equitably balancing the complicated trade-offs that no single nation-state can do by fiat. The private sector and civil society have shown they can lead the way. In order for an American-inspired vision of Internet governance to triumph, however, the United States must continue to promote multistakeholder governance, while pushing back against ill-conceived laws and regulations that would threaten the free and open Internet.

INTRODUCTION

This inquiry comes at a particularly timely moment, as we stand at a historic crossroads in global Internet governance policy. The road we are currently on — governed by the principles set forth in the Clinton administration's *Framework for Global Electronic Commerce* — has seen the flourishing of digital communications over the past quarter century. At their core, these policies, such as ensuring the free flow of information across borders and governance via multistakeholder-driven compromise, are built on a foundation of quintessential American values: openness, transparency, free expression, free and open markets, and a culture of tolerance and respect for ecumenicalism.

Turning off this road would lead us toward a theory of Internet governance that is inherently antithetical to those American values. The core vision of this alternative path, as articulated by Chinese President Xi Jinping in a speech on April 20, is a government-dictated, command-and-control system of governance. As President Xi describes it, the Internet of the future is one in which "the government … will manage, enterprises … will carry out responsibilities, society … will supervise, and netizens … will self-discipline."[i] He continued:

> *We must strengthen online positive propaganda, unequivocally adhere to the correct political direction, and the guidance of public opinion; and, oriented by values, we must use the Thought of Socialism with Chinese Characteristics for a New Era and the spirit of the 19th Party Congress to unite and bring together millions of netizens; deeply develop education on ideals and beliefs; deepen propaganda and education on Socialism with Chinese Characteristics for a New Era and the Chinese Dream; vigorously foster and practice the Socialist Core Value View; advance innovation in online propaganda ideas, concepts, forms, methods, measures, etc.; grasp these with timeliness and efficiency; build concentric circles online and offline; generate better social cohesion and consensus; and lay down a common intellectual basis for the united struggle of the entire Party and the whole nation. We must consolidate the main responsibilities of Internet enterprises. We can absolutely not let the Internet become a platform for the dissemination of harmful information, or a place where rumours spread that create trouble. We must strengthen self-discipline in the Internet sector, muster the vigor of all netizens, and mobilize forces on all sides to participate in governance.*[ii]

Such a future portends the end of the free and open Internet. As Samm Sacks, a senior fellow at the Center for Strategic and International Studies, noted in a recent article in *The Atlantic*, the ramifications of this vision of global Internet governance supplanting the existing American-led order are profound:

> *This alternative would include technical standards requiring foreign companies to build versions of their products compliant with Chinese standards, and pressure to comply with government surveillance policies. It would require data to be stored on servers in-country and restrict transfer of data outside China without government permission. It would also permit government agencies and critical infrastructure systems to source only from local suppliers.*[iii]

"The problem with China's model," Sacks notes, "is that it crashes headlong into the foundational principles of the [I]nternet in market-based democracies: online freedom, privacy, free international markets, and broad international cooperation."[iv] She goes on:

> *China's control-driven model defies international openness, interoperability, and collaboration, the foundations of global [I]nternet governance and, ultimately, of the [I]nternet itself. The 21st Century will see a battle of whether it is the China model or the more inclusive, transparent, collaborative*

principles that underpinned the [I]nternet's rise that come to dominate global cybersecurity governance.[v]

In order to ensure the latter model of Internet governance prevails, the American government must continue to play a leading role in its defense. To that end, these comments will address the National Telecommunications and Information Administration (NTIA) notice of inquiry "seeking comments and recommendations … on its international [I]nternet policy priorities for 2018 and beyond."[vi] Parts I-IV will answer specific questions (listed under each header) associated with each of the primary policy issues: (1) The Free Flow of Information and Jurisdiction, (2) Multistakeholder Approach to Internet Governance, (3) Privacy and Security, and (4) Emerging Technologies and Trends. Part V will then summarize the recommendations from Parts I-IV before concluding.

PART I: THE FREE FLOW OF INFORMATION AND JURISDICTION

Expansive interpretations of consumer harm, antitrust analysis that relies on ill-defined market boundaries, and amorphous rules governing privacy are all potentially crippling to an interconnected world that remains fragile. Theories surrounding "data price gouging" and laws like the General Data Protection Regulation (GDPR), while not rising to the potential threat posed by more overt state-backed calls for control, are nonetheless dangerous policy prescriptions that hold the potential to balkanize the global Internet.

The Trojan Horse Triumvirate: GDPR, "Data Price Gouging," and Digital Trade

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

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?

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

E. What should be the role of all stakeholders globally — governments, companies, technical experts, civil society and end users — in ensuring free expression online?

As discussed above, the primary challenge to the continued free flow of information online, particularly speech, is the potential for the "control-driven model" of global Internet governance to usurp the existing order. However, other national laws and regulations could similarly impede cross-border information flows, to the significant detriment of not only U.S. companies, but free expression more broadly. The following section will detail three separate laws and policies that could act as Trojan horses that would, whether intended or not, fragment the global Internet.

GDPR

The European Union's (EU) recently-implemented GDPR rules, for example, have already had a considerable effect on the continent's digital economy.[vii] Some of their negative economic effects include:

1. "**Members of the Fortune 500 will spend a combined $7.8bn** to avoid falling foul of Brussels' [GDPR], according to estimates compiled by the International Association of Privacy Professionals (IAPP) and [accounting firm] EY. This equates to **an average spend of almost $16m each**."[viii]

2. "Of the companies who said they have finished preparations [for GDPR], **88% reported spending more than $1 million** on GDPR preparations and **40% reported spending more than $10 million**."[ix]

3. Fines for GDPR infringement can reach up to "**€20 million or 4% of the business's total annual worldwide turnover**."[x]

4. "Since the early hours of May 25, **ad exchanges have seen European ad demand volumes plummet between 25 and 40 percent** in some cases, according to [Digiday] sources."[xi]

While the GDPR is effectively a tariff on the EU technology sector and a compliance tax on its American counterpart, the rules also had a chilling effect on trans-Atlantic speech. Some digital publishers were taken offline after GDPR went into effect (e.g., Instapaper, *Los Angeles Times*, *Chicago Tribune*, and A&E Networks websites); others switched to stripped down EU-only versions without images or illustrations (e.g., *USA Today* and NPR); and at least one major publisher, *The Washington Post*, started charging readers more for a GDPR-compliant subscription.

As Professor Daniel Lyons, a visiting fellow at the American Enterprise Institute, noted in recent commentary,[xii] these actions were driven by "concerns that imperfect implementation would trigger liability," with the unfortunate outcome being a reduction in net information exchange between the United States and EU. Looking to the future of a post-GDPR Europe, Lyons goes on to note that:

> *The chilling effect on digital products available to European consumers could be significant. Even if companies are not actively marketing to European residents, they may have European visitors interacting with their webpage, taking advantage of marketing offers, or subscribing to newsletters. If these interactions result in retention of personally identifiable information, the company is subject to the GDPR. The ease with which a company may find itself bound, coupled with the cost of compliance and potentially draconian penalties for violation, creates strong incentives for companies to withdraw — aggressively — from European markets.*[xiii]

Underlying the GDPR is a belief that nebulous privacy regulations, whatever their shortcomings, are still preferable to more targeted and gameable rules. Better to be too expansive and ensure maximal privacy protections for the broadest number of people, even if the costs to economic growth, free expression, and consumer welfare are substantial. Ultimately, these rules represent a clear value trade-off, heavily weighing in favor of privacy to the detriment of all other considerations. (It should be noted, however, that while the GDPR places a heady premium on privacy, it is unclear – and indeed, heavily contested – whether the rules have had, or will have, any substantive positive impact for user privacy.) A system that prioritizes privacy over all else not only jeopardizes economic growth and innovation, but also an individual's right to free expression.

The Department of Commerce and NTIA should push back on overzealous privacy-protections regimes like GDPR in all international fora and negotiations. Although privacy is certainly an important value to defend internationally, the level of protection afforded to individuals' right to online privacy comes with trade-offs, not least of which is a thriving digital economy. The United States should continue embracing a sectoral-based privacy regime where harms, if they materialize, are contextualized according to the type of information implicated. NTIA should everywhere and always maintain a commitment to balancing privacy with other rights and values, and push back against attempts to commit the United States to any legal regime that might imperil not only the country's thriving technology industry, but other rights and values, such as freedom of speech.

"Data Price Gouging"

In an interview with *The New York Times*, Andreas Mundt, the president of Germany's Federal Cartel Office (FCO), said, "The Facebook case is really about excessive pricing vis-à-vis the consumer."[xiv] Mundt was arguing that, because Facebook is the dominant firm in the social networking market, it has been essentially "data price gouging" its users by requiring them to share valuable personal data in exchange for using the platform's free social networking services.

In a recent research brief, the Niskanen Center examined this ongoing investigation into Facebook's purported abuse of its market power. We showed that there are a multitude of problems inherent in the FCO's new theory of consumer exploitation:

> *Determining a data-price is but one of two interrelated problems. The other is adjudicating what constitutes "your" data; what information you "own" about yourself, as well as how, or whether, that ownership inheres in a legal, economic, and technical framework. Quantifying the value of data is difficult in isolation; when paired with the necessity of resolving age-old questions of epistemic philosophy, the task is near-impossible.*[xv]

In addition to these data-pricing concerns, the FCO will also need to wrestle with how to define the relevant market for Facebook to determine how dominant it actually is. For instance, if Facebook is actually in the attention industry — which encompasses all of entertainment — then its market share will be a fraction of what it is in the social networking market. These problems are thorny for antitrust regulators to grapple with and could lead to socially inefficient regulatory interventions for many technology companies beyond Facebook.

Digital Trade

Trade agreements should reiterate America's commitment to online-intermediary liability protections. Content delivery networks (CDN) — linked servers that enable faster and more secure delivery of content to users — are one type of intermediary that Internet users interact with every day but are not aware of unless they stop working. As the Niskanen Center argued in 2016 comments submitted to the United States Trade Representative (USTR), such services actually help facilitate a safer and more secure online experience for users. And contrary to claims made by the Motion Picture Association of America (MPAA),[xvi] CDNs are not "notorious markets" operating "in blatant violation of the law" by failing to effectively police intellectual property infringement. As we noted:

> *There are many benefits of utilizing CDNs, not least of which are the significant cost savings on storage and bandwidth when compared to central server streaming networks. Whatever benefits some actors participating in notorious markets may reap from CDN services, the mere possibility of a technological tool being used for ill is not justification enough for it to be held liable for the actions of users. As online content becomes more interactive and bandwidth-intensive, a more distributed network will increasingly become the most architecturally beneficial approach to optimizing user experience and services.*[xvii]

CDNs like Cloudflare and Akamai are increasingly valuable enablers of the digital ecosystem, and NTIA, in conjunction with USTR, should rebuff erroneous claims from the MPAA and others suggesting these services are aiding and abetting "notorious markets." More broadly, NTIA should explicitly defend the intermediary liability protections that allow CDNs and other online services to facilitate the free exchange of speech and ideas online.[xviii] We concluded our previous comments by saying that "any effort to expand

enforcement obligations … to these CDN companies can only harm the health of the online ecosystem; it would chill free speech, cripple innovation of an evolving Internet architecture, and serve to make millions of websites less secure."[xix]

The CLOUD Act: Bringing Order to Chaos

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?

G. In which international organizations or venues might NTIA most effectively advocate for the free flow of information and freedom of expression? What specific actions should NTIA and the U.S. Government take?

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

Until recently, a primary challenge to the free flow of digital data was the lack of a comprehensive legal framework for addressing cross-border data access by law enforcement. With the recent passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act,[xx] the United States has taken an important step in updating the law to accommodate the unique extraterritoriality issues raised by a digital world.[xxi] As passed, the law permits the Attorney General, contingent on the "concurrence" of the Secretary of State, to enter into bilateral cross-border data-sharing agreements with foreign governments, subject to a determination that the foreign government, among other things:

1. "Demonstrates respect for the rule of law and principles of nondiscrimination";[xxii]
2. "Adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights," which includes, among other things, "freedom of expression, association, and peaceful assembly";[xxiii] and
3. "Demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet."[xxiv]

Additionally, the law stipulates that a foreign government entering into such an agreement with the United States may not use any order issued under the terms of the agreement "to infringe freedom of speech."[xxv] Although the Departments of State and Justice are the ultimate decision-makers in determining a country's eligibility for entering into a data-sharing agreement, the Department of Commerce and NTIA may have a collaborative role to play in contributing to these determinations. Given its long history of dealing with international Internet policy the Department of Commerce and NTIA likely have unique and valuable insights to offer the Attorney General and Secretary of State.

NTIA should thus help inform future deliberations on such agreements by providing the Departments of Justice and State insights and information gleaned from international discussions with Internet stakeholders.

PART II: MULTISTAKEHOLDER APPROACH TO INTERNET GOVERNANCE

In theory, the Department of Commerce and NTIA are limited in actively setting and promoting international policy for the Internet. In practice, however, by working with and through other organizations, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance

Forum (IGF), NTIA can lend significant support to ongoing efforts aimed at providing multistakeholder governance, while continuing to promote American values.

The Framework for Global Electronic Commerce

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 *Framework for Global Electronic Commerce* (hereafter the *Framework*) was released by the Clinton administration in 1997 as a directive to government agencies for how to approach regulation of the inchoate Internet in their respective policy areas.[xxvi] In a retrospective published fifteen years after the *Framework* was first implemented, Adam Thierer, a senior research fellow at the Mercatus Center at George Mason University, said:

> *[The* Framework *was] a paradigm for how cyberspace should be governed that remains the most succinct articulation of a pro-liberty, market-oriented vision for cyberspace ever penned. It recommended that we rely on civil society, contractual negotiations, voluntary agreements, and ongoing marketplace experiments to solve information age problems. In essence, they were recommending a high-tech Hippocratic oath: First, do no harm (to the Internet).*[xxvii]

Collectively, the set of principles underlying the *Framework* is a form of "soft law" (as opposed to "hard law"). Soft law includes using a multistakeholder approach to governance which incentivizes compromise and helps build trust among all parties.[xxviii] This was the perfect foundation to enable the explosive growth and success of the Internet in its early years. The Department of Commerce echoed this philosophy recently in its green paper, *Fostering the Advancement of the Internet of Things*:

> *Over the past few decades in the United States, the role of government largely has been to establish and support an environment that allows technology to grow and thrive. Encouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making, have been integral elements of the government's approach to technology development and growth. Following a review of public comments, meetings with stakeholders, and the public workshop, it is clear that while specific policies may need to be developed for certain vertical segments of IoT, the challenges and opportunities presented by IoT require a reaffirmation rather than a reevaluation of this well-established U.S. Government policy approach to emerging technologies.*[xxix]

The paper went on to note that "the Department reaffirms its commitment to the policy approach that has made the United States the leading innovation economy. This approach is reflected in the 1997 Framework for Global Electronic Commerce, and has been maintained across all subsequent Presidential administrations."[xxx] We agree that this is the right approach for the Internet, the Internet of Things, and for most other emerging technologies.

Accountability, Trust, and "Governance Learning"

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?

C. Are the existing accountability structures within multistakeholder Internet governance sufficient? If not, why not? What improvements can be made?

As Arizona State University legal scholars Gary Marchant and Braden Allenby have noted, soft law and multistakeholder governance practices are most applicable to those areas where technology is rapidly and continually outpacing the ability for regulators and policymakers to keep up.[xxxi] A telling indicator of when a multistakeholder approach might be suitable, they note, is a policy arena in which "governments, industry, and the public are struggling to realize the promising benefits – and manage the disruptive impacts — of one rapidly emerging technology after another."[xxxii] The multistakeholder process — a core tenet of the soft law system in emerging technology governance — aims to achieve a type of co-regulation that is fundamentally defined not by bureaucratic decision-making, but by an open and transparent consensus-building exercise driven by the private sector, civil society, non-governmental organizations, and others.[xxxiii] That is why the *Framework* was so successful in promoting the growth and proliferation of the Internet: it prioritized flexible, adaptive, nonbinding standards of governance over top-down, command-and-control rules.

In the field of emerging technologies and the Internet, soft law and multistakeholder governance practices provide numeours benefits over older models of regulatory action,. These benefits include:

1. Providing opportunities for "governance learning" by establishing a baseline quasi-regulatory structure that can be built upon;

2. Serving as a political steam valve to insulate policymakers from the need to act haphazardly and preemptively prior to known harms;

3. Introducing greater transparency, vested adaptivity, and enhanced responsiveness into rulemaking proceedings;

4. Amplifying trust and incentivizing compromise among stakeholders, thereby injecting heightened resiliency into the governance process; and

5. Creating more opportunities for equitably balancing innovation and the public interest without being excessively precautionary.[xxxiv]

Taken together, the benefits of a multistakeholder governance approach to emerging technologies in general, and the Internet in particular, far outweigh the attendant costs.[xxxv] (As a general response to Question B above, we would direct NTIA to a forthcoming law journal article in the *Colorado Technology Law Journal* authored by Ryan Hagemann, Adam Thierer, and Jennifer Skees: "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future." For ease of reference, we have submitted a copy of that journal article along with these comments.)

The NTIA and the Department of Commerce would be well-served by continuing to employ soft law governance mechanisms in their approach to the Internet and emerging technologies. Further, NTIA should reiterate its commitment to these principles at every opportunity. In every international multistakeholder discussion, forum, or engagement, the Department of Commerce and NTIA should commit to a policy of unceasing and relentless reaffirmation of these principles and how their propagation helped create the modern digital economy.

Staying the Course on the IANA Transition

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

It has been almost two years since the Department of Commerce ended its contract with ICANN and the U.S.-based nonprofit organization took full control of the IANA functions.[xxxvi] Since the transition, ICANN has continued to be an excellent steward of the Internet's unique identifiers. This is not surprising given the

multi-decade planning that went into preparing for the transition. As a testament to these preparations, at the time of the handover there was bipartisan and international support for moving oversight of this critical function to a private-sector organization operating on a multistakeholder governance model.

Technical experts and policymakers said this transition would cause no disruption to Internet users and preserve a level playing field for the Internet worldwide.[xxxvii] As we near the two-year milestone, Assistant Secretary David Redl's decision to review the transition is commendable. First, in considering whether to unwind the IANA Stewardship Transition, it is important to remember how widespread the support was for following through on the commitment to make this change.

New America's Open Technology Institute released a paper arguing in favor of the transition.[xxxviii] The American Enterprise Institute published an article calling it the "responsible" choice.[xxxix] Immediately following the change, the Electronic Frontier Foundation said, "Now that the transfer of oversight has gone through, life will go on pretty much as it did before, with the exception that a broader group of people will have the formal responsibility of ensuring that the DNS root zone is being administered according to community-developed policies"[xl]

Critics' greatest fears about the transition have proven to be unfounded. There have been no significant disruptions to users and the stability of the multistakeholder system is strong.[xli] Authoritarian regimes did not take control of Internet governance. Even at the time of the transition, the repressive regimes themselves recognized that this was not a radical change from the status quo ante. In criticizing the proposed transition, Rashid Ismailov, the Russian vice minister of telecom and mass communication, reportedly said, in effect, "that ICANN would remain a U.S. corporation and the functions of the NTIA would just be resolved within the ICANN procedures, and be totally laid on U.S. ground."[xlii]

In announcing its support for the transition, the Information Technology and Innovation Foundation argued that "if anything, threatening the legitimacy of the multistakeholder model will strengthen the hand of those nations that wish to gain greater control over the Internet — the main concern of those still opposing the transition — since they will be able to argue that the U.S. government still holds undue influence over ICANN, better justifying their own interventions."[xliii]

In February of this year, the Brookings Institution published a review of the transition by Joe Kane, a technology policy associate at R Street Institute, and Milton Mueller, a professor at Georgia Tech School of Public Policy, in which they said:

> *That transition was the right move at the time and remains so today … ICANN is an imperfect organization with politics and problems of its own. But the transition led to dramatic improvements in ICANN's accountability and corporate governance … Accepting stewardship by ICANN is still preferable to reverting to the NTIA, which would bring injurious consequences for global Internet freedom. For those who value global Internet freedom, the former is the only option.*[xliv]

The verdict is clear: Internet stakeholders are largely satisfied with the transition and the Commerce Department would be committing an unforced error if it attempted to reverse its decision.

PART III: PRIVACY AND SECURITY

The giant machine that is the global digital economy depends on trust to oil the gears. Advances in privacy tools and security protocols have enabled users to trust one another enough to transact — without ever seeing each other in the flesh. These gains in online commerce should not be taken for granted and need to be defended by smart public policy.

Addressing Cybersecurity Threats

A. In what ways are cybersecurity threats harming international commerce? In what ways are the responses to those threats harming international commerce?

In 2015, 42 percent of small businesses in the United States were victims of a cybersecurity attack, according to a survey by the National Small Business Association.[xlv] Often, these attacks occur in the form of botnets, a mass network of computers infected with malicious software to spam legitimate Internet users. In aggregate, these attacks are one of the leading harms to international commerce. But what can we do to prevent them?

According to congressional testimony from Daniel Castro, the vice president of the Information Technology and Innovation Foundation, in order to reduce the number and severity of these attacks, the United States should "reform its national cybersecurity policy to move away from an emphasis on relative offensive capabilities and instead prioritize absolute defensive capabilities, including prosecuting cybercrime."[xlvi] The government could improve the defensive capabilities of the private sector by codifying the process by which it shares zero-day exploits with firms. Furthermore, as detailed in regulatory comments filed last year by the Niskanen Center, the Commerce Department could promote the use of cybersecurity insurance and extend public-private information sharing regimes.[xlvii] These steps could significantly reduce the harm posed by botnets.

However, some policy recommendations for dealing cybersecurity threats come with negative unintended consequences. For example, paring back intermediary liability protections for online service providers and content delivery networks would do more harm than good. The business models of these providers and networks, in which they connect users around the world and host content at little or no cost, are only economically viable if the government defends their protection from liability for third-party content. In fact, many of the new products created by these networks can promote online security. It would be a mistake to snuff out those innovations with well-intentioned but poorly-designed changes to liability protections.[xlviii]

Strong encryption is a more general solution to a wide variety of cybersecurity threats on the Internet. As the *The Atlantic* noted in its coverage of our 2015 paper on the economic benefits of encryption, "The $40-plus trillion online banking industry, for example, would have been 'significantly stunted' without strong cryptography… and the online purchases that in 2013 totaled more than $3.3 trillion depended on encryption for trust and security."[xlix] In the few years since the paper's release, the digital economy has only grown larger and, with it, so has the importance of encryption. The paper's conclusion still holds true today: "The Internet is the lifeblood of the modern digital economy; encryption protocols are the white blood cells. The health of the Internet ecosystem depends on the proliferation of strong encryption."[l]

Competing Visions of Privacy

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

Rules like GDPR – ill-conceived though they may be – are usually manifestations of a desire for more robust online privacy protections. Unfortunately, as the GDPR rollout demonstrates, apportioning broad, overly-prescriptive, one-size-fits-all regulations to govern large, diverse, and complex economic ecosystems will inevitably result in unintended (though often foreseeable) consequences – not only for firms and economic agents but also for free speech and expression. While they may be crafted with the best of intentions, far-reaching rules and regulations fail to account for the inherent dynamism of market economies, and such rules can never fully or accurately account for the future opportunities and challenges that will arise.

As Craig Mundie, senior advisor to the CEO of Microsoft, aptly noted in a 2014 article for *Foreign Affairs*, had the United States embraced an all-encompassing GDPR-style regulatory approach to privacy in the early days of the Internet, its growth would have almost certainly been stymied:

> *If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.*[li]

And indeed, just as the Internet of the 1990s did not resemble the Internet of the 2000s, neither will the Internet of the 2020s necessarily resemble the Internet of today. As the technologist Martin Geddes once wrote, the Internet is just a prototype.[lii]

In that spirit, as a general matter, NTIA should affirm and support the United States' long-standing approach to regulating privacy sectorally as a superior alternative to more general and comprehensive rules. This approach has long served the country well, and has made the U.S. technology sector the envy of the world. In international venues, NTIA should point to the United States as an example of how countries can craft balanced privacy regulations that address particularized harms while promoting economic growth in digital markets. The agency should further affirm that the United States remains committed to regulating privacy concerns domestically, and eschew any attempt to bind the country to amorphous and unenforceable international standards or agreements.

Furthermore, NTIA should consider promoting the taxonomy of information harm put forward by the Information Technology and Innovation Foundation in their comments submitted to the Federal Trade Commission (FTC) last year:

> *When evaluating how consumers can be harmed through the misuse of their information, the FTC should use a more detailed typology for information and the harms that result from that information. In addition, as discussed above, limiting data collection and data sharing is an inappropriate method to reduce informational injury in many situations. Consumers are better served by more targeted rules that address specific harms. Only by narrowly tailoring these definitions and pursuing informational injury cases based on demonstrated harm can the FTC both protect consumer privacy and advance innovation.*[liii]

For all of these policies, the only international venues that are "appropriate to address questions of digital privacy" are multistakeholder fora that aim to promote voluntary, nonbinding standards. NTIA's participation in such fora, however, should always, and explicitly, be premised on noncommittal conditions of involvement. And as the *Framework*'s first principle pronounced (and the Department of Commerce recently reaffirmed, as discussed *supra*), in all such venues, it should be the official policy of NTIA and the U.S. government that "the private sector should lead," and "governments should encourage industry self-regulation and private sector leadership where possible."[liv] American firms and civil society should thus serve as the tip of the spear in any international multistakeholder efforts that aim to "address" policies, issues, or concerns related to online or digital privacy. NTIA can serve as an effective advocate and convener of multistakeholder processes, but the private sector and civil society should continue to lead in this arena.

PART IV: EMERGING TECHNOLOGY AND TRENDS

The Internet allows emerging technologies to diffuse throughout the world at record speed. The benefits to innovation from the information superhighway are clear, but the ability to share data faster than ever also enables spam bots and intellectual property infringement. Fortunately, some emerging technologies, such as machine learning, can also be used to fight back against these scourges. International Internet policies should mitigate these risks while also maximizing the fruits of innovation.

As the Commerce Department works with international organizations in crafting these policies, it would be wise to make use of its in-house expertise: the Emerging Technology and Research Advisory Committee (ETRAC). The Committee can use its institutional knowledge to emulate the best practices of previous governance regimes and ensure an optimal balance between risk mitigation and benefit maximization.

Automated Content Filtering

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

Ongoing debates surrounding foreign election interference have increasingly cast the specter of expanded use of automated content take-down systems. The use of so-called content recognition systems (CRS)[lv] can certainly help assist online service platforms in combating the spread of everything from "fake news" to extremist terrorist content, while also balancing the needs of content creators and copyright holders. These systems often use artificial intelligence — specifically, machine learning algorithms — to automate the take-down process, which makes it cost effective for platform owners to police their networks for malicious or stolen content.

However, even though this technology is promising, mandating the implementation of CRS or predicating intermediary liability protections for online service providers on their use should be a red line set by U.S. representatives in any international discussions.[lvi] Online intermediaries may choose different methods or levels of content moderation based on their community's unique needs, and blanket requirements would ignore the "particular circumstances of time and place"[lvii] to the detriment of economic dynamism.[lviii]

Promoting Innovation

B. In which international venues should conversations about emerging technology and trends take place? Which international venues are the most effective? Which are the least effective?

C. What are the current best practices for promoting innovation and investment for emerging technologies? Are these best practices universal, or are they dependent upon a country's level of economic development? How should NTIA promote these best practices? For any response, commenters may wish to consider describing specific goals and actions that NTIA, the Department, or the U.S. Government in general, might take (on its own or in conjunction with the private sector) to achieve those goals; the benefits and costs associated with the action; whether the proposal is agency-specific or interagency; the rationale and evidence to support it; and the roles of other stakeholders.

The U.S. government should use the soft law governance principles outlined above as its approach to regulating emerging technologies beyond the Internet. A multistakeholder model with nonbinding guidance and industry-led best practices is the best way forward for many of our most promising technologies, including regenerative medicine, the Internet of Things, autonomous vehicles, drones, supersonic flight, and

commercial space travel. Each of these technologies has the potential to radically improve the lives of Americans and policymakers should use what they have learned from Internet governance to inform how they approach these game-changing innovations.

Lastly, the Commerce Department should capitalize on the ETRAC, which is already housed at the Department but has been underutilized in the past. This committee is a vital store of institutional knowledge and could be be leveraged to accelerate the Department's policy priorities once they have been established.[lix] It is especially important that, given its role, the Committee maintains its commitment to the principles outlined in the *Framework*.[lx]

PART V: SUMMARY OF RECOMMENDATIONS

To ensure that international Internet policy continues to remain consistent with American values, the Department of Commerce and NTIA should consider the following recommendations, as discussed *supra*:

The Free Flow of Information and Jurisdiction

1. **Maintain a steady and unapologetic commitment to the American approach to privacy governance, balancing digital privacy with other rights and interests, such as freedom of expression and the growth of the digital economy;**
2. **Express support for digital competition policies rooted in a defense of the consumer welfare standard, rather than broad, ill-defined, and economically unsound claims (such as "data price gouging" or "excessive data pricing") that might justify unwarranted interference in the market;**
3. **Defend the value of, and advocate for, online intermediary liability protections as an important legal framework for safeguarding free speech and digital trade; and**
4. **Offer recommendations to, and share information with, the Departments of Justice and State in future deliberations over bilateral data-sharing agreements pursuant to the CLOUD Act.**

Multistakeholder Approach to Internet Governance

1. **Continuously reaffirm the Department of Commerce's commitment to the *Framework* and related soft law governance principles;**
2. **Emphasize the need for the private sector and civil society to lead on international multistakeholder efforts, while reiterating NTIA's limited role as a convener and advocate for the multistakeholder governance process; and**
3. **Stay the course on the successful IANA Stewardship Transition.**

Privacy and Security

1. **Affirm and support the United States' long-standing approach to regulating privacy sectorally;**
2. **Reiterate the value of secure encryption for promoting trust in, and the growth of, the digital market; and**

3. **Affirm the United States's commitment to regulating privacy concerns domestically, while abstaining from accepting amorphous and unenforceable international standards or agreements, even if only nonbinding.**

Emerging Technology and Trends

1. **Defend intermediary liability protections for online service providers and CDNs; and**

2. **Leverage the institutional knowledge housed at the Emerging Technology and Research Advisory Committee to help inform international conversations regarding new technologies.**

CONCLUSION

In announcing the *Framework*, President Bill Clinton began by saying:[lxi]

> *The invention of the steam engine two centuries ago and the harnessing of electricity ushered in an industrial revolution that fundamentally altered the way we work, brought the world's people closer together in space and time, and brought us greater prosperity. Today, the invention of the integrated circuit and computer and the harnessing of light for communications have made possible the creation of the global Internet and an electronic revolution that will once again transform our lives.*

The global Internet and the electronic revolution did indeed transform our lives. But that transformation is far from over. If we are to avoid the grim possibility of global Internet governance with Chinese characteristics, we must embrace anew the principles underlying the Clinton administration's *Framework*:

1. "The private sector should lead."

2. "Governments should avoid undue restrictions on electronic commerce."

3. "Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce."

4. "Governments should recognize the unique qualities of the Internet."

5. "Electronic commerce on the Internet should be facilitated on a global basis."[lxii]

This national framework applies as much, if not more so, at the international level. As the fifth principle notes, electronic commerce takes place on the global level and governance policy should be aligned with that reality. The rest of the principles remain as true today as when they were first put forward. Commerce, either electronic or analog, still needs a consistent, predictable, and simple legal environment to maximize the benefits to human beings worldwide. The private sector has shown that it can lead the way and, if the government can avoid undue restrictions, we can maintain an open and free Internet.

NTIA has an important role to play in these efforts. By working in concert with other departments and agencies, NTIA can help lead a united front in international negotiations to ensure the continuation of an American vision for the Internet – where freedom, openness, and collaborative governance trump state-sponsored repression, control, and censorship.

We would like to thank NTIA for the opportunity to comment on this issue and look forward to continued engagement on this and other topics.

[i] Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference," New America, 30 April 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/.

[ii] *Ibid.*

[iii] Samm Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *The Atlantic*, 18 June 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

[iv] *Ibid.*

[v] *Ibid.*

[vi] Department of Commerce, National Telecommunications and Information Administration, "International Internet Policy Priorities," *Federal Register*, Vol. 83, No. 108 (Tues., June 5, 2018), pp. 26036 - 26038, https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-international-internet-policy-priorities-06052018.pdf.

[vii] Adam Thierer, *GDPR Compliance: The Price of Privacy Protections*, Technology Liberation Front, 9 July 2018, https://techliberation.com/2018/07/09/gdpr-compliance-the-price-of-privacy-protections/.

[viii] https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc.

[ix] "Pulse Survey: GDPR budgets top $10 million for 40% of surveyed companies," PriceWaterhouseCoopers, https://www.pwc.com/us/en/services/consulting/library/general-data-protection-regulation-gdpr-budgets.html.

[x] "What if my company/organisation fails to comply with the data protection rules?," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en.

[xi] Jessica Davies, *GDPR mayhem: Programmatic ad buying plummets in Europe*, Digiday, 25 May 2018, https://digiday.com/media/gdpr-mayhem-programmatic-ad-buying-plummets-europe/.

[xii] Daniel Lyons, "GDPR: Privacy as Europe's tariff by other means?," American Enterprise Institute, 3 July 2018, https://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/.

[xiii] *Ibid.*

[xiv] Natasha Singer and Sapna Maheshwari, "European Regulators Ask if Facebook Is Taking Too Much Data," *The New York Times*, 24 April 2018, https://www.nytimes.com/2018/04/24/technology/facebook-data-europe-investigations.html.

[xv] Ryan Hagemann, *Data Price Gouging: A Stalking Horse for a Neo-Brandeisian Antitrust Doctrine?* (Washington, D.C.: Niskanen Center, 8 May 2018), p. 6, https://niskanencenter.org/wp-content/uploads/2018/05/Brief-Data-Price-Gouging_-A-Stalking-Horse-for-a-Neo-Brandeisian-Antitrust-Doctrine_.pdf.

[xvi] Joanna McIntosh, *Comments of the Motion Picture Association of America, Re: Request for public comment on the 2016 Special 301 Out of Cycle Review of Notorious Markets*, Docket No. USTR-2016-0013, submitted October 7, 2016, p. 11, available at https://www.regulations.gov/document?D=USTR-2016-0013-0007. ("Some hosting providers allow sites to hide behind a content delivery network (CDN). A CDN is typically used to effectively and efficiently deliver content to a global user base by placing servers all around the world that cache the pages of the website. One of the by-products of using a CDN is that they mask the true IP and hosting provider of a website. An example of a CDN frequently exploited by notorious markets to avoid detection and enforcement is Cloudflare. Cloudflare is a CDN that also provides reverse proxy functionality. Reverse proxy functionality hides the real IP address of a web server. Given the central role of hosting providers in the online ecosystem, it is very concerning that many refuse to take action upon being notified that their hosting services are being used in clear violation of their own terms of service prohibiting intellectual property infringement and, with regard to notorious markets such as those cited in this filing, in blatant violation of the law.")

[xvii] Ryan Hagemann, *Comments submitted to the United States Trade Representative in the Matter of: A Rebuttal to "A Request for Comment on the 2016 Special 301 Out-of-Cycle Review of Notorious Markets,"* Niskanen Center, Docket No. USTR-2016-2013, (submitted October 20, 2016), https://niskanencenter.org/wp-content/uploads/2016/10/NiskanenCenter_USTRCommentsNotoriousMarketsRebuttal.pdf.

[xviii] Ryan Hagemann, *Comments submitted to the National Telecommunications and Information Administration in the Matter of: Promoting Stakeholder Action Against Botnets and Other Automated Threats*, Docket No. 170602536-7536-01, (submitted July 28, 2017), https://www.ntia.doc.gov/files/ntia/publications/niskanencenter_comments_botnets_ntia.pdf.

[xix] Ryan Hagemann, *Comments submitted to the United States Trade Representative in the Matter of: A Rebuttal to "A Request for Comment on the 2016 Special 301 Out-of-Cycle Review of Notorious Markets,"* Niskanen Center, Docket No. USTR-2016-

2013, (submitted October 20, 2016), https://niskanencenter.org/wp-content/uploads/2016/10/NiskanenCenter_USTRCommentsNotoriousMarketsRebuttal.pdf.

[xx] CLOUD Act (S. 2383, attached to Pub. L. 115-141, 23 March 2018).

[xxi] Curt Levey, et. al., *Coalition Letter to House and Senate Leadership RE: The Clarifying Lawful Overseas Uses of Data Act*, (Feb. 13, 2018), http://bit.ly/cloudcoalitionletter. ("By providing clear guidelines, the CLOUD Act takes several steps to avoid international conflicts of law and protect the privacy of citizens across the globe while prioritizing the fight against international crime and terrorism. Because it facilitates U.S. entry into bilateral agreements with other governments, the proposed legislation would encourage government-to-government cooperation. The CLOUD Act updates the law to make it clear that U.S. warrants and similar legal processes issued for data held by service providers will likely reach data stored overseas. At the same time, the legislation would also give these providers rights to raise international comity concerns that would require a judge to determine if competing government interests weigh in favor of compelling the provider to turn over the requested data.")

[xxii] 18 U.S.C. § 2523(b)(1)(B)(ii) (2018).

[xxiii] 18 U.S.C. § 2523(b)(1)(B)(iii)(III) (2018).

[xxiv] 18 U.S.C. § 2523(b)(1)(B)(vi) (2018).

[xxv] 18 U.S.C. § 2523(b)(4)(E) (2018).

[xxvi] White House, *A Framework for Global Electronic Commerce*, (1997), [hereafter the *Framework*], https://clintonwhitehouse4.archives.gov/WH/New/Commerce/summary.html.

[xxvii] Adam Thierer, *15 Years On, President Clinton's 5 Principles for Internet Policy Remain the Perfect Paradigm*, Forbes, 12 Feb. 2012, http://bit.ly/2KZ3mnn.

[xxviii] Ryan Hagemann, Adam Thierer, and Jennifer Skees, "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future," *Colorado Technology Law Journal* (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539.

[xxix] National Telecommunications and Information Administration, *Fostering the Advancement of the Internet of Things*, (Jan. 12, 2017): p. 2, https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[xxx] *Ibid.*, 40.

[xxxi] Gary E. Marchant and Braden Allenby, "New Tools for Governing Emerging Technologies," *Bulletin of the Atomic Scientists*, Vol. 73 (2017).

[xxxii] *Ibid.*, 108.

[xxxiii] Hagemann, Thierer, and Skees, "Soft Law for Hard Problems," 15.

[xxxiv] Ryan Hagemann, "New Rules for New Frontiers: Regulating Emerging Technologies in an Era of Soft Law," *Washburn Law Journal*, Vol. 57, No. 2, (Spring 2018), pp. 244-255, http://washburnlaw.edu/publications/wlj/issues/57-2.html.

[xxxv] *Ibid.*, 255. (These costs can potentially include, among other things: "(1) Diminished long-term legal clarity, given the lack of common law adjudication of soft criteria and the soft law systems they engender; (2) [s]ubjecting agencies to criticism that such approaches ignore the rule of law and provide new avenues by which industry interests can engage in regulatory capture, thereby undercutting institutional legitimacy; and (3) [o]pening the door to policy entrepreneurs motivated by hostility to technology and progress, ideologically dogmatic policy preferences, or nefarious intentions.")

[xxxvi] "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends," ICANN Announcements, 1 Oct. 2016, https://www.icann.org/news/announcement-2016-10-01-en.

[xxxvii] Stephen D. Crocker, Patrick Falstrom, and Ram Mohan, "Opposition gets facts wrong on ICANN's security committee and the IANA transition," *The Hill,* 21 Sept. 2016, http://thehill.com/node/297035.

[xxxviii] David G. Post and Danielle Kehl, *Controlling Internet Infrastructure: The "IANA Transition" and Why It Matters for the Future of the Internet, Part I* (New America's Open Technology Institute, Apr. 2015), http://bit.ly/2LpPw9M.

[xxxix] Shane Tews, "The IANA transition: Creating a responsible outcome," TechPolicyDaily, 26 Sept. 2016, http://www.aei.org/publication/the-iana-transition-creating-a-responsible-outcome/.

[xl] Jeremy Malcolm, "Oversight Transition Isn't Giving Away the Internet, But Won't Fix ICANN's Problems," Electronic Frontier Foundation, 3 Oct. 2016, http://bit.ly/2LpbB80.

[xli] Joe Kane and Milton Mueller, "U.S. government should not reverse course on internet governance transition," TechTank, 7 Feb. 2018, http://brook.gs/2BK7nqD.

[xlii] Monika Ermert, "ICANN Meeting in Marrakesh: More Hiccups On Way to IANA Transition," Intellectual Property Watch, 3 Aug. 2016, http://www.ip-watch.org/?p=46069.
[xliii] Daniel Castro, "The IANA Transition Is Not Perfect, But Congress Should Approve It Anyway," Innovation Files, 14 Sept. 2016, https://itif.org/node/6515.
[xliv] Kane and Mueller, *supra note* 37.
[xlv] National Small Business Association, "2015 Year End-Economic Report" (2016), http://bit.ly/2uHO630.
[xlvi] "Testimony of Daniel Castro Before the Senate Committee on Small Business and Entrepreneurship," 25 Apr. 2018, http://www2.itif.org/2018-small-business-cybersecurity-castro.pdf.
[xlvii] Ryan Hagemann, *Comments submitted to the National Telecommunications and Information Administration in the Matter of: Promoting Stakeholder Action Against Botnets and Other Automated Threats*, Docket No. 170602536-7536-01 (submitted July 28, 2017), https://www.ntia.doc.gov/files/ntia/publications/niskanencenter_comments_botnets_ntia.pdf.
[xlviii] *Ibid.*
[xlix] Kaveh Waddell, "How Much Is Encryption Worth to the Economy?" *The Atlantic*, 9 Nov. 2015, http://bit.ly/2NVhuvD.
[l] Ryan Hagemann and Josh Hampson, *Encryption, Trust, and the Online Economy: An Assessment of the Economic benefits Associated With Encryption*, Niskanen Center, 9 Nov. 2015, https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.
[li] Craig Mundie, "Privacy Pragmatism," *Foreign Affairs*, Vol. 93, No. 2 (March/April 2014), p. 517, http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.
[lii] Martin Geddes, "The Internet is just a prototype," 4 April 2015, http://www.martingeddes.com/?p=1094.
[liii] Daniel Castro and Alan McQuinn, "Comments submitted to the Federal Trade Commission RE: Informational Injury Workshop, Project No. 175413," Information Technology and Innovation Foundation, 27 Oct. 2017, http://www2.itif.org/2017-informational-injury-comments.pdf.
[liv] The *Framework*.
[lv] These refer to any number of software technologies or algorithms (including "filtering" and "fingerprinting" systems) that are involved in the automated identification and/or take-down of copyright-infringing materials online. *See* Evan Engstrom and Nick Feamster, *The Limits of Filtering: A Looks at the Functionality & Shortcomings of Content Detection Tools*, (San Francisco: Engine, March 2017), http://www.engine.is/the-limits-of-filtering; *See also* Regina Zernay and Ryan Hagemann, *ACES in the Hole? Automated Copyright Enforcement Systems and the Future of Copyright Law*, Research Paper (Washington, D.C.: Niskanen Center, June 6, 2017): p. 36, http://bit.ly/niskanen_aces.
[lvi] *Ibid.*, 36. ("As a result, it is imperative that policymakers refrain from advocating for additional conditionality set on the safe harbor provisions of the [Digital Millennium Copyright Act]. In particular, safe harbor provisions for [online service providers] should not be conditioned on the use of [content recognition systems], automated or otherwise.")
[lvii] Friedrich A. Hayek, "The Use of Knowledge in Society," *American Economic Review* (1945), https://www.econlib.org/library/Essays/hykKnw.html.
[lviii] Zernay and Hagemann, *ACES in the Hole?*.
[lix] Ryan Hagemann and Joshua Hampson, "Comments submitted to the Bureau of Industry and Security in the Matter of: Emerging Technology and Research Advisory Committee Meeting," (submitted March 14, 2017), http://bit.ly/niskanen_etrac.
[lx] *Ibid.*
[lxi] "Text of the President's Message to Internet Users," White House Office of the Press Secretary, 1 July 1997, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/message.html.
[lxii] The *Framework*.