Testimony of Christopher M.E. Painter

Before the United States Senate Committee on Commerce, Science and Transportation
Subcommittee on Communications, Technology, Innovation and the Internet

Hearing on "The Internet and Digital Communications: Examining the Impact of Global Internet Governance"

July 31, 2018

Chairman Wicker, Ranking Member Schatz, members of the Senate Subcommittee on Communications, Technology, Innovation and the Internet, it is a pleasure to appear before you today to discuss the impact of global Internet governance and policies on American businesses, end users and the U.S. policy of promoting and maintaining an open, interoperable, secure and reliable communications and information infrastructure that is the foundation for economic prosperity, innovation, social growth and the exercise of human rights. For over twenty-six years I have devoted my life to cyber and Internet issues, serving as a federal prosecutor specializing in cybercrime, a senior official at the Department of Justice and the FBI, a Senior Director of Cybersecurity Policy at the National Security Council and, most recently, as the first Coordinator for Cyber Issues at the Department of State. I have continued to work on these issues since leaving the federal government, among other things, serving as a Commissioner on the Global Commission for the Stability of Cyberspace and a Board member of the Center for Internet Security.

My role as Coordinator for Cyber Issues at the State Department was the first such office established in a foreign ministry. There are now over twenty-five such offices in foreign ministries around the globe. In recognition of the cross-cutting and interdependent nature of cyber and Internet issues — including economic, human rights and security issues — my former office had a broad mandate, and worked with components across the Department, the interagency, the private sector, civil society and other stakeholders, to advance the U.S. vision of an open and secure cyberspace. In my six and a half years as Coordinator, I worked to help realize the many benefits of cyberspace while combatting the ever mounting technical and policy threats we face. For purposes of this hearing I will focus on some of the policy challenges, including threats to the multi-stakeholder system of Internet governance, threats to freedom of expression and other human rights online, challenges relating to cybersecurity and stability, and the threat of inconsistent or misguided regulatory or policy regimes that threaten to fragment the global Internet and undermine its economic and social value. I will also make some recommendations to address these challenges.

First, I would like to make some general observations. The policy threats we face, though distinct, are also inter-related and have economic, human rights and security elements. For example, when China claims absolute sovereignty over its cyberspace and erects a digital wall around its territory in the name of security, that has profound economic and human rights implications. Similarly, when a country enacts a regulatory regime for cybersecurity, privacy or some other goal, it could, intentionally or unintentionally, significantly affect the free flow of information over the Internet and act as market barrier. It is vital therefore that our response to these challenges not be siloed but be coordinated — bringing together the full range of departments, agencies and other stakeholders to advance an integrated and strategic U.S policy. Second, cyber and Internet issues are now being debated in virtually every country and every international and regional organization (including the G7, G20, OECD, ITU, OAS, ASEAN, OSCE and multiple committees in the UN devoted to security, human rights, economic and development issues). Indeed, I believe we have reached an inflection point, where the issues discussed and the decisions reached in these multiple forums will have a major impact on the future of the Internet and cyberspace — determining whether we can all continue to benefit from this incredible technology based on the free flow of information and multi stakeholder governance or whether the growing technical and policy threats will lead to fragmentation and undermine its incredible potential.

Accordingly, advancing the U.S. vision of cyberspace, including U.S. commercial interests, requires unprecedented U.S. international engagement and strategic U.S. leadership. Both structure and resources need to be addressed to enable the level of engagement that is now required.

Challenges

Though I won't attempt to catalogue the all of the many policy challenges we face in cyberspace, some of those relevant to this hearing include:

Maintaining Multi-stakeholder Internet Governance

The U.S. has long advocated a multi-stakeholder approach to Internet governance that is characterized by a transparent, bottom-up, consensus driven process in which all stakeholders — including governments, the private sector, civil society, the technical community and academia — participate on an equal footing. This relatively novel approach is responsible for the tremendous growth of the Internet around the world and has enabled the free flow of information, vast commercial opportunity, innovation, resilience and robust technical evolution. Among others, the organizations responsible for the technical operation of the Internet and multi stakeholder discussions of policy issues include the International Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF) and the Internet Governance Forum (IGF). Though these and other institutions can and should be further strengthened, through, for example, more inclusive participation, they have served the community well. Nevertheless, for many years, a number of more repressive countries, and Russia and China in particular, have sought to impose greater state control on the Internet and have pushed for an intra-governmental body, such as the United Nations, to take over technical governance and Internet policy. In part, their push for intra-governmental control is based on their desire to control information and expression that they believe can threaten regime stability. Imposing a multilateral government control mechanism would fundamentally change the Internet as we know it, and would seriously affect the free flow of information, human rights online and thwart innovation and growth. Fortunately, the U.S. working with like-minded partners around the world, has succeeded so far in pushing back against these efforts so far but they are likely to continue to be raised in the future. For example, the Plenipotentiary of the International Telecommunications Union, a meeting that occurs every four years to chart the ITU's mandate, is happening this fall. The ITU is a UN body that is made up of country representatives who largely have telecommunications expertise and, although other stakeholders can participate in discussion, they are excluded from decisions — a far cry from a multi-stakeholder body. In past meetings, some governments have tried to expand the ITU's scope to include technical Internet governance and the ITU has often itself has tried to expand its role beyond its area of expertise to deal with a number of cyber and Internet policy issues. The U.S. must continue to be on high alert to these and other efforts and strategically work with other countries and stakeholders to thwart attempts to undermine the multi-stakeholder approach that has served us well.

Ensuring Freedom of Expression and Human Rights Online

The global Internet has enabled unprecedented communication and expression and that free flow of information has had tremendous human rights and economic benefits. Yet despite the economic and social benefits of an open Internet, some states see that openness, as discussed above, as a threat to regime stability and seek to curtail it by censorship, repression and restricting Internet access. The Freedom on the Net Report 2017, published by Freedom House, details a sobering picture of declining Internet freedom around the world and the actions of many repressive countries to control and manipulate speech and content. In addition, network shutdowns are a growing problem around the world where a government restricts the public's access to the Internet during an election or other political event. Some cybersecurity policies can also have human rights implications. While the U.S. encourages countries to have cybersecurity strategies that fully incorporate human rights and economic interests, some states, like China and Russia have "cybersecurity" policies and laws that are aimed at controlling discourse and dissent. These countries both claim "absolute sovereignty" in cyberspace and do not recognize that international human rights transcend international borders. Restrictive policies curtailing the free flow of information have both negative human rights and economic impacts. The U.S. has been a leader in advancing Internet freedom in the past including helping found the Freedom Online Coalition, a group of thirty countries dedicated to advocating for these issues in multiple forums around the world. The U.S. must continue to lead to guarantee both human rights and economic benefits of the Internet.

Fighting Data Localization

A number of countries have enacted or are considering data localization mandates that require data belonging to residents, companies or entities of that country to be stored in that country. Though these laws or policies arise in part from concerns about surveillance or difficulty in accessing data for law enforcement investigations when stored abroad, and are often described as privacy or security measures, they instead, in many cases, act as trade barriers and mechanisms to enable greater state control of content. Data localization requirements, essentially mandating that U.S. and other global providers construct data centers in localities around the world, are not scalable or economically practical, and are particularly anticompetitive to new or smaller players. These mandates also completely undercut many of the benefits of the cloud architecture including increased efficiency, access and the possibility of greater security. Moreover, some states, like Russia, enact such requirements to better control dissent. Of course, there are legitimate concerns that some states have raised with respect to access to data. When data is stored in the U.S., our electronic privacy laws make access for a foreign government difficult in a law enforcement investigation even if the crime and participants all were in that country. The U.S. has attempted to address this recently through the Clarifying Lawful Overseas Use of Data (CLOUD) Act. Though negotiating bilateral agreements pursuant to this law should be a priority, the U.S. must also continue to push back against data localization in all of its engagements.

Addressing Potentially Conflicting, Misguided or Unfair Regulatory and Legal Regimes

Countries and multilateral bodies around the world are enacting or considering regulatory, policy or legal regimes dealing with some aspect of cyberspace and the Internet. Among other things, these frameworks attempt to address online privacy, cybersecurity, market access and emerging technology such as the Internet of Things (IoT). Though some of these measures are meant to address real concerns in a country or region, they often have unintended (and sometimes intended effects) that extend well beyond their borders. In some cases, if the locally developed standard is made the global default, there is a risk of impacting freedom of speech or other strongly held U.S. values. In other cases, there is the risk of a multiplicity of conflicting regimes that serve to fragment Internet commerce and create a confusing landmine for global companies. And in some cases, the policies are explicitly aimed at encouraging "indigenous innovation" and act as market access barriers.

For example, many of China's laws and regulations, including its Cybersecurity Law, are deliberately vague but have broad implications for data localization, mandatory testing, cooperation with Chinese authorities, forced technology transfer and market access in China. Though China presents this and other laws and policies as best practices for cybersecurity, it can act as a significant impediment to U.S. and other companies doing business in China, as well as serious human rights concerns, and will create even further barriers if adopted by other countries as a best practice.

The European Union has been addressing a number of issues in cyberspace including privacy and cybersecurity. The General Data Protection Regulation (GDPR) is now the law in the E.U. Among other things, it creates privacy related requirements for entities processing E.U. citizen data that extends to most U.S. Internet and global companies. Yet, extraterritorial application of the GDPR may create conflicting obligations for U.S. companies. For instance, the GDPR enshrines the "right to be forgotten" that mandates that E.U. individuals can force service providers to remove certain information about themselves. However, such a mandate may well conflict with the First Amendment right of freedom of expression and unduly infringe public access. In cybersecurity terms, though the GDPR creates a standard for cybersecurity protections of personal data, and has a carve out for data that must be shared for network defense purposes, it has had an unintended consequence in potentially rendering WHOIS, an important tool used by industry and law enforcement to combat online crime, less accessible and useful. The E.U. has also been working on a Cybersecurity Act that mandates a mostly voluntary certification regime for Internet connected devices. This law has evolved significantly with a lot of U.S. and other industry input and could end up becoming a de-facto global standard.

Other countries and regional organizations are also addressing a myriad of other issues including cyber breach reporting and potential policies around the Internet of Things. Unless these efforts are compatible, or at least interoperable, and unless they adopt a risk based approach, they will pose significant challenges for U.S. global entities.

Promoting a Secure and Stable Cyber Environment

The future viability of the Internet as a platform for commerce and social good depends on that platform's security and the long term stability of cyberspace. Threats by nation states, organized criminal groups and other bad actors threaten to undermine government, business, consumer and individual confidence in the Internet and networked technologies. Moreover, a number of recent cyberattacks and intrusions amply demonstrate that malicious cyber activity can have large economic impact.

With respect to cybercrime, consistent laws and strong enforcement are paramount. The U.S. has championed the Budapest Convention on Cybercrime which creates consistent substantive laws and procedures. Sixty countries have now joined that Convention. Russia has long opposed Budapest and, instead, is set to promote a new cybercrime convention in the United Nations this fall. A new convention will take many years to negotiate, be less strong than the Budapest Convention and will likely seek to deal with content issues that are protected in the U.S. More importantly, if countries wait for a new convention, it will undermine the real need for every country to address this issue now.

On cybersecurity, it is in the U.S. interest for countries to have comprehensive national strategies that are drafted with multi stakeholder input and take into account security, economic and human rights perspectives and for countries to have institutions and the ability to cooperate with the U.S. in sharing information and addressing online threats. With respect to both cybercrime and cybersecurity, targeted capacity building is important to building the capability of other countries to work with us in addressing online threats.

Malicious nation-state activity, such as Russian interference with our elections and democratic processes around the world or their sponsorship of the economically destructive NotPetya ransomeware worm, requires both a short term deterrence strategy and a long term effort to achieve cyber stability. On deterrence, we need to do a much better job of imposing timely and credible costs on adversaries, particularly nation states, who do us harm in cyberspace. On stability, it is important that we continue to advance internationally a framework of cyber stability that includes voluntary rules of the road, or norms, for nation state conduct. The U.S. has made a good deal of progress on that front, including getting agreement from many countries on voluntary norms that countries should not attack critical infrastructure in other countries in peacetime and should not steal trade secrets or intellectual property through cyber means to benefit their commercial sector. The Commission for the Stability of Cyberspace, on which I serve as a Commissioner, is a multi-stakeholder group that has sought to advance this work, including by proposing two norms: 1. That state and non state actors should not take actions that substantially damage the general availability of the public core of the Internet and 2. That state and non state actors should not allow cyber operations intended to disrupt the technical infrastructure supporting elections. Getting other countries to embrace these voluntary norms and a larger stability framework that includes the application of international law in cyberspace and certain confidence building measures, will pay both national security and economic dividends but more needs to be done.

Some Thoughts on the Way Ahead

Increased Coordinated International Engagement

Given that every country and virtually every international and regional multilateral organization is now dealing with some aspect of cyberspace or the Internet, my overarching recommendation is that it is imperative that the U.S. government and U.S. stakeholders step up diplomatic engagement on these issues around the world and that this is made a true national priority. This recommendation is also echoed in a number of the submissions to the recent Notice of Inquiry on International Internet Policy Priorities issued by the National Telecommunications and Information Administration (NTIA). To up our game on international engagement requires enhanced structure, resources, and a whole of government cross-cutting strategy.

I applaud the continued efforts of my former colleagues at State, Commerce and other agencies, but I believe those efforts have been hampered by the lack of a sufficiently high-level office at the State Department and the recent abolition of the Cyber Coordinator position at the White House. On the first, as I noted above, my former office, among many other things, facilitated coordination across the government and helped provide high level representation with other governments to advance U.S. policies on a range of issues. I commend the House and Senate efforts to restore, strengthen and institutionalize my former office. The House passed the Cyber Diplomacy Act several months ago and the Senate Foreign Relations Committee recently voted a companion bill out of committee. I am particularly pleased that these were bi-partisan efforts reflecting the bi-partisan nature of most of these issues. Hopefully, the Department of State will take action on this matter soon.

Given the cross-cutting nature of these issues, international engagement on them requires a whole of government approach that leverages not just the State Department and the Commerce Department but the full range of U.S. agencies in a coordinated and strategic way. In the past, that coordination has been significantly boosted by the Cyber Coordinator at the National Security Council. Though the coordinator sat in the NSC and had a focus on security issues, he also brought together and worked with other parts of the White House, including the National Economic Council, the Office of Management and Budget, the Office of Science and Technology Policy, and the interagency on a range of policy issues including Internet governance. Indeed, when the position was first suggested in the Cyberspace Policy Review in 2009, it was to be dual hatted between the NSC and NEC to fully account for the wide range of issues in cyberspace. In any event, the loss of that high-level position, coupled with the at least temporary demotion of my prior office, complicates interagency coordination and also sends the unfortunate signal to both our friends and our adversaries that the Administration does not really prioritize these issues.

Resources are another important consideration. For example, assuming my old office is resurrected, it still needs sufficient personnel and funding to be effective. This importantly includes funding for capacity building that was severely cut last year. Capacity building can take many forms, including working with foreign governments and emerging leaders on aspects of Internet governance or regulatory policy, helping countries enact appropriate laws and national strategies, and working with countries to boost their ability to combat cybercrime and have strong cybersecurity policies and institutions. For a relatively small amount, targeted capacity building not only helps the U.S. by helping other countries gain the capabilities to work with us, but it also has the benefit of helping to win the support of developing countries for our vision of the Internet and cyberspace. Convincing these countries that we want to help and that an open, interoperable and secure Internet benefits them, is particularly important in enlisting their support in the growing array of multi-lateral bodies that are now addressing Internet and cyber issues.

It is also important for the private sector, civil society and other stakeholders to continue to engage in these efforts and enhance their participation. Many companies and civil society groups already work in a variety of international forums and their contributions are invaluable. And, I fully understand there are significant resource and time constraints both for the private sector and especially civil society given the number of places discussions and decisions are taking place. Nevertheless, given what is at stake we must find ways to help increase participation.

Finally, it is important that the U.S. has a high-level cross-cutting, integrated strategy that leverages all relevant government agencies, outside stakeholders and like-minded countries to deal with the many challenges we face internationally and helps direct and prioritize our engagements. The U.S. International Strategy for Cyberspace issued in 2011 helped guide and integrate U.S. policy and agency actions across economic, security, and human rights issues. The overarching goal was that "[t]he United States will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace." Much has happened since then and there are many new challenges. Although the current Administration, by Executive Order, mandated a number of important reports and recommendations from agencies largely related to cybersecurity, no larger or comprehensive strategy that, among other things, weaves those recommendations together, has yet been released.

Strengthening Multi-stakeholder Internet Governance Institutions

There are a number of efforts underway to strengthen existing multi-stakeholder Internet Governance institutions to make them more transparent, effective and inclusive that we should continue to support. These efforts are important not only to make these institutions more capable but also to insulate them from those countries trying to impose intergovernmental control over the Internet. In addition, sustained and increased participation by governments and other stakeholders in these institutions is also important and increases their legitimacy. Among other things, the U.S. government should work to sustain and strengthen the Internet Governance Forum. The IGF provides a valuable forum for stakeholders around the world to engage in discourse on the full range of Internet and cyber issues. Although its mandate was extended for ten years just two years ago, it has suffered from a lack of sustained funding, a decrease in attendance by senior government officials and the private sector, and issues related to its continuity from year to year. The U.S. is and should continue to be an advocate for this forum but should also help sustain and improve it. The U.S. has helped fund the IGF in the past and should do so again now and encourage other contributions. The U.S. should also encourage and help facilitate strong senior participation particularly by senior U.S. officials and other senior stakeholders. Moreover, the U.S. can play a key role in helping the IGF address any perceived or actual shortcoming without making it a decisional body or fundamentally changing its character.

Filling the Void and Showing Leadership

If the United States wants to drive the global conversation or have its policies serve as a global standard it has to lead by example. That has been done in the past when, for example, we made cyber issues a diplomatic priority or when the National Institute of Standards and Technology promulgated their Cybersecurity Framework in partnership with industry and very effectively promoted it around the globe. Part of this is the high level international engagement I discuss above but part of it is promoting concrete alternatives. For example, with respect to privacy, the Obama Administration proposed a Consumer Privacy Bill of Rights and there was legislative action that was started, though not completed, to put them into law. Affirmative privacy legislation would help push back on misperceptions by some in Europe that the U.S does not care about privacy and can serve as an attractive alternative for countries who are now considering privacy legislation of their own. Federal data breach legislation has also languished for some time even though every state has their own version of breach legislation and other countries are moving forward with their own proposals. I am not suggesting legislation is the only way to show leadership and any legislation needs to solicit stakeholder input and balance potentially competing interests, but the U.S. needs to present an affirmative vision and concrete alternatives to policies we don't believe serve our interests or the interests of an open and secure Internet.

Accelerate Negotiations under the CLOUD ACT

The CLOUD Act coupled with an executing bilateral agreement takes away one of the traditional justifications for data localization. Accordingly, accelerated negotiations of bilateral agreements under the Act should be encouraged and resourced. Of course, the countries or groups of countries with whom such agreements are negotiated must have adequate due process and privacy protections and these agreements will not prevent governments from mandating localization if they want to do so to repress their citizenry or to impose a market barriers, but the potential availability of these agreements can make a real difference with a number of partners. In addition, work should continue and resources should be allocated to streamline and speed up the Mutual Legal Assistance process.

Promote Cybersecurity, Cybercrime and Stability Efforts to Increase Trust and Security

Although this may be beyond the jurisdiction of this Subcommittee, programs designed to increase international efforts to combat cybercrime and promote cybersecurity should be encouraged and resourced as these programs make cyberspace more profitable and secure for our businesses and safer for our citizens. This includes capacity building efforts to ensure countries have strong laws, policies and institutions; promotion of basic cyber hygiene measures; enhanced operational information sharing enabling prosecutions and enabling collective response to shared threats; and increased deterrence of malicious state actors. Finally, the U.S. should continue to demonstrate leadership on efforts to secure the long term stability of cyberspace and engage with other countries and other stakeholders on this important issue.

Thank you for the opportunity to testify today on this important and timely issue, I look forward to your questions.