
Internet 2020: The Next Billion Users

Lawrence E. Strickling[†]

I. INTRODUCTION

I am honored to have the opportunity to preface this edition of *CommLaw Conspectus* and discuss the Internet policy priorities we are addressing at the National Telecommunications and Information Administration (“NTIA”).

Last November, President Obama held an unprecedented town hall meeting with students in Shanghai, China. In response to a question about the openness of the Internet, the President called himself a “big believer” in technology and the free flow of information. He referred to the lack of censorship by our government as a “tradition” and said “the fact that we have a free Internet or unrestricted Internet access is a source of strength, and . . . should be encouraged.”

One of NTIA’s top priorities is to develop policy approaches and build consensus to realize the President’s vision of an Internet that is open for innovation and social progress, both domestically and globally. The Internet’s open, end-to-end architecture and the freedom of individuals to make full use of that architecture have fueled tremendous creativity, innovation, and economic growth. Preserving, enhancing, and increasing everyone’s access to an open, global Internet is an urgent policy priority for the Obama administration and for other governments and communities all around the world.

[†] Lawrence E. Strickling has served as Assistant Secretary for Communications and Information at the United States Department of Commerce since his confirmation by the United States Senate on June 25, 2009. In this role, Strickling serves as Administrator of the National Telecommunications and Information Administration (NTIA), the executive branch agency that is principally responsible for advising the President on communications and information policies, managing the federal use of electromagnetic spectrum, performing cutting-edge telecommunications research and engineering, formulating and advocating for U.S. positions on international communications and information technology policy matters, and administering infrastructure and public telecommunications facilities grants. The author wishes to thank Daniel J. Weitzner, Associate Administrator for Policy Analysis and Development, NTIA, for his significant insights and contributions in the composition of this article and to Dennis J. Amari for additional support.

To that end, NTIA and others within the Department of Commerce recently announced the formation of an Internet Policy Task Force whose mission is to identify leading public policy and operational challenges in the Internet environment. While the Task Force is still in the process of receiving and analyzing input from many stakeholders, the Internet's history and its many institutions can teach us much about how to face today's pressing Internet related public policy challenges.

II. THE CHALLENGE OF SUCCESS: INTERNET POLICY 3.0

In order to ensure the sustainability and continued growth of the Internet, it is imperative that we preserve the trust of all actors on the Internet. If users do not trust that their personal information is safe on the Internet, they will not use it. If content providers do not trust that their content will be protected, they will stop putting it online. If large enterprises fear that their network will be breached over the Internet, they will be reluctant to take full advantage of the ability to link to their suppliers and customers. If foreign governments do not trust the Internet governance systems, they will threaten to balkanize the Domain Name System, jeopardizing the worldwide reach of the Internet. At NTIA, we describe this set of challenges in terms of developing an "Internet Policy 3.0."

Confronting the challenges of Internet Policy 3.0 will require the use of a broad spectrum of tools. Some challenges can be addressed purely by the private sector. Many will require cooperation between the private sector, civil society, and the technical community with government either as convener or cajoler. In just a few cases, we may have to resort to laws or regulation to establish fundamental rules of the road. To understand how to deploy these different tools, we can learn a lot from the institutions and approaches that led to the creation of the Internet and the Web.

A. Technical Institutions

The Internet Society, the Internet Engineering Task Force ("IETF") and the World Wide Web Consortium ("W3CA") are rightfully credited for developing the open platform architecture that has been the basis of the social and economic innovation that characterizes the Information Society today. Not only did these multi-stakeholder organizations build the technical foundations of the Internet, but they also pioneered innovative social institutions, embodied in the working groups and architecture boards of the IETF and W3C, that enabled people all over the world to contribute to and shape the Internet we have today.

B. Administrative Institutions

The viability of the Internet's multi-stakeholder model was tested early with the need to develop a globally scalable, open system to coordinate critical name and number resources. In what was then an ambitious experiment, the Internet Corporation for Assigned Names and Numbers ("ICANN") was created in 1998 to coordinate the technical management of the domain name system ("DNS"). A very thorough consultative process provided the basis for the development of ICANN and its core principles, which include: preserving the stability of the Internet; promoting market mechanisms to support competition and consumer choice; ensuring private sector leadership with bottom-up policy processes; and encouraging broad international representation.

C. Voluntary, Enforceable Best Practices

Online privacy is an example of the vital role that voluntary, global, multi-stakeholder activity can play in addressing Internet policy questions. Back in the mid-1990s, NTIA played a leading role, along with the Federal Trade Commission ("FTC"), in exploring options to address new online privacy issues. It is certainly the case that policymakers wanted to avoid squelching innovation and no one was really sure what privacy challenges would emerge. So, no sweeping privacy legislation was enacted. Rather, a combination of self-regulatory actions taken by the online industry, encouraged by the Clinton administration, and backed by broad enforcement authority at the FTC, took form in the late 1990s.

At the FTC's urging, major Web sites agreed to post privacy policies explaining how they use personal information. While the FTC has no specific authority to make rules about privacy, it does have broad responsibility under Section 5 of the Federal Trade Commission Act to investigate and punish companies engaging in 'unfair or deceptive' trade practices. In this case, if a company posts a privacy policy and then proceeds to use personal information in more intrusive ways, it can be held accountable by the FTC. At the same time, the then-nascent online advertising industry developed a code of conduct governing the use of personal information. That code became enforceable under the same 'unfair and deceptive' authority.

So, while the FTC did not engage in a traditional rulemaking, it formed part of a hybrid public-private system in which there are a clear set of rules that are enforceable by the FTC. As privacy scholars Deirdre Mulligan and Ken Bamberger recently wrote, this type of dynamic, hybrid system in which both private and public stakeholders participate may well yield actual privacy practices that are more responsive to evolving consumer privacy expectations than would a traditional rulemaking system.

D. Laws

At the far end of the continuum of tools available to address Internet policy issues is the enactment of laws. While we must encourage the type of collaborative process that led to the privacy protections of the 1990s, we should not conclude that the Internet is beyond the reach of the law. One historical example is instructive.

Very early in its life, when less than one percent of the world's citizens used the Internet, openness of the Internet was nearly nipped in the bud by an act of Congress. Included in the Telecommunications Act of 1996 were far-reaching Internet censorship provisions, known as the Communications Decency Act, which threatened to stifle both protected speech and legitimate commerce on the new medium. Those provisions were struck down by the U.S. Supreme Court. But in the very same act, Congress also included a provision—Section 230—that most believe has contributed significantly to foster the growth and evolution of the Internet. In fact, it has been described as one of the most important guarantors of free speech on the Internet and considered to be responsible for securing the vibrant culture of freedom of expression that exists today on the Internet.

Section 230 provides Internet intermediaries immunity from liability arising out of content created by third-parties. This limitation on liability has enabled the creation of innovative sites that host content provided by others without requiring those services to monitor every single piece of content uploaded to their sites. However, Section 230 does not discourage responsible cooperation toward compliance with laws online; if illegal activity occurs online, such as the misuse of personal private information, the theft of a copyrighted work, or the intrusion into someone else's system or network, these provisions pose no impediment to the enforcement of our criminal laws or the pursuit of justice.

III. INTERNET 3.0 PUBLIC POLICY ISSUES

The adaptation of these models to the current challenges of Internet Policy 3.0 is our focus at NTIA and that of the Department's Internet Policy Task Force. The issues on our agenda include the following:

Privacy policy: The challenge is to enable the development of innovative new services and applications that will make intensive use of personal information, but at the same time protect users against harm and unwanted intrusion into their privacy. The Internet Policy Task Force released a broad-ranging Notice of Inquiry to solicit public comment on April 23, 2010. The notice seeks views on the continued vitality of the hybrid regulatory model combined with enforceable codes of conduct and backstop regulatory enforcement by the FTC; the usefulness of this model; and the extent to which the model, if ex-

tended, will promote greater flexibility in the cross-border flow of personal information while assuring trust mechanisms among governments to vindicate the rights of their citizens globally.

Child Protection and Freedom of Expression: This inquiry focuses on understanding, as more children go online, how we can ensure proper targeting of law enforcement resources against serious crime while remembering that the most important line of defense against harmful content is the well-informed and engaged parent or teacher. Later this year, the Online Safety Technology Working Group, created by Congress and convened by NTIA, will issue a report on the state of the art in child protection strategies online. In addition, as recommended by the Federal Communications Commission ("FCC") in the National Broadband Plan, we will consider the need to continue a working group in this area.

Cybersecurity: The Internet Policy Task Force also is examining how best to meet the security challenges posed by the global Internet, such as the need for increased law enforcement and private sector technology innovation while ensuring respect for citizen privacy and the protection of civil liberties. Of particular attention is how these objectives can be assured, particularly as they relate to improving industry preparedness for cyber attacks.

Copyright Protection: The protection of copyrighted works and intellectual property on the Internet, while also preserving the rights of users to access lawful content is the focus of this inquiry. NTIA and our sister agency, the U.S. Patent and Trademark Office, are beginning a comprehensive consultation process that will help the Administration develop a forward-looking set of policies to address online copyright infringement in a balanced, Internet-savvy manner.

Internet Trade and the Free Flow of Information: The focus of this inquiry is how best to work with U.S. businesses and other entities to understand the economic impact of restrictions on global flows of information to U.S. trade and investment. The Internet Policy Task Force has just begun exploring this issue and will be reaching out to stakeholders for their views in the coming months.

IV. CONCLUSION

Every one of these issues shares two common characteristics. First, they are global in scope, raising questions about whether a single government or actor could provide comprehensive solutions. Second, they arise in the context of fast-changing technologies, marketplaces, and evolving patterns of social interaction, causing many who study these issues to doubt that traditional government regulatory processes can provide adequate, flexible responses. Never-

theless, to preserve trust on the Internet, it is not an option for governments to merely sit by and hope that these issues will take care of themselves. But that does not mean we should take a sharp turn away from the current approach to the Internet that the U.S. government has championed over the years. Rather, we should take a careful look at the unique multi-stakeholder, public-private models that have led to the success of the Internet and the World Wide Web and determine how best to bolster them to meet today's challenges.

At the opening of the third decade of Internet policymaking, we are at an 'all hands on deck' moment. Today's policy challenges are far broader than we have previously faced. In addition to continuing the necessary technical innovation of the Internet, the Internet community needs to work with governments and other stakeholders to share their knowledge about how to build flexible, sustainable, global multi-stakeholder institutions that can help the world face the social and public policy challenges of the global Internet environment.