THE REMARKABLE INTERNET GOVERNANCE NETWORK—PART II

Moving to the Next Era

Don Tapscott
Executive Director
Global Solution Networks

and

Lynn St. Amour
President and CEO
Internet Matters

with

Steve Caswell
Principal Researcher
Global Solution Networks

The multi-stakeholder ecosystem that governs the Internet has been enormously effective in developing and implementing the standards and policies required for this unprecedented communications medium to work. This success was reflected in the March 14, 2014 announcement by the US Commerce Department's National Telecommunications and Information Administration of its intent to "transition key Internet domain name functions to the global multi-stakeholder community."

As the Internet penetrates every aspect of economic, social and political life, there is a new set of broader issues that must be addressed. The Internet governance network is well positioned to take the next steps, and address the thorny policy issues ranging from privacy, security and neutrality, to spam, pornography and intellectual property.

GLOBAL SOLUTION NETWORKS

Table of Contents

The Idea in Brief

On March 14, 2014, the US Commerce Department's National Telecommunications and Information Administration (NTIA) announced its intent to transition key Internet domain name functions to the global multi-stakeholder community that governs the Internet. This is both a natural step forward and a powerful statement that the multi-stakeholder model is effective, legitimate and should be supported by countries around the world. It also signals that this ecosystem needs to take the next steps to promote the evolution of Internet governance.

In just 25 years, since the invention of the World Wide Web gave it a killer app, the Internet has emerged as the most important communications network in history. The Net has become an essential part of the fabric of commerce, innovation, learning, entertainment and the everyday life of billions of people around the world.

Many of the Internet's powerful capabilities, however, come with potential side effects. Email networks can be flooded with unwanted spam. Credit card fraud and identity theft can threaten every user on the Internet. Vulnerable users can easily become the victims of cyberbullying on social networks. And then there is the concern about spyware, malware or computer viruses.

Individuals and businesses worldwide are concerned with protecting the intellectual property rights they have worked hard to create, while everyone faces privacy threats from governments who may spy on Internet activity (Big Brother) and corporations that track Internet behavior for targeted advertising purposes (Little Brother). Individuals, furthermore, are often unaware of the privacy implications of their own Internet use (Baby Brother).

Pornography and even worse ills, including cybersex trafficking, have invaded the Internet. Finally, and this may be the most troubling problem of all, governments responsible for fighting terrorism or maneuvering to hold onto power are putting Internet filters in place, gathering information on what their citizens are doing or trying to control what citizens can see and do on the Net.

These problems need to be put into perspective. Spam is still more of a nuisance than a serious problem to most users. Only a small percentage of the more than 2.5 billion Internet users worldwide have been negatively impacted by issues like credit card fraud, intellectual property theft, cyberbullying, identity theft or government spying. There is a benefit from organizations tracking our digital footprints because the data enables better customized services.

Nevertheless, while problems may be perceived or experienced by a minority, even a small percentage of 2.5 billion users becomes a large number in absolute terms, which poses a challenge to the Internet governance

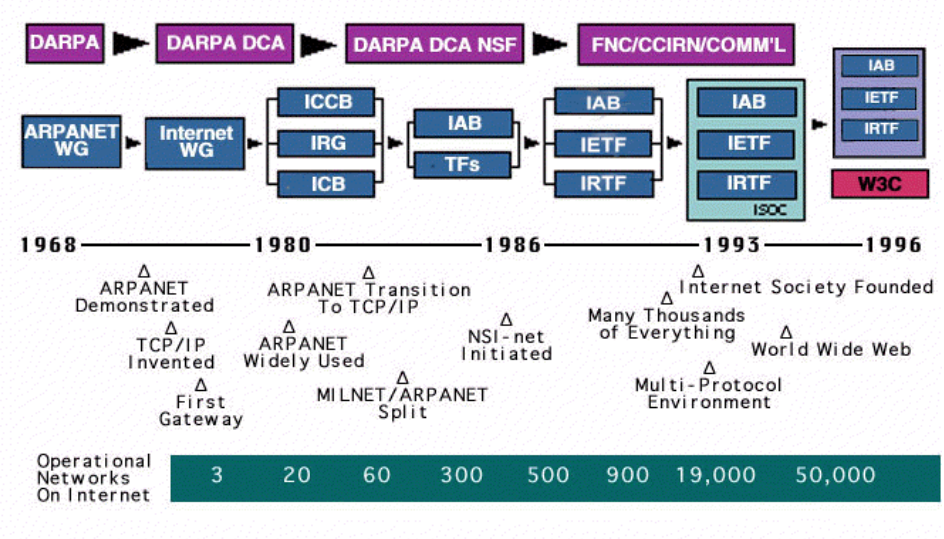
network. This document—a companion to our report on the evolving roles and structure of the Internet governance network[1]—identifies a taxonomy of issues that will challenge Internet governance. Many, if not all, of these issues will require technical, political and educational components, some of which may be developed and delivered by global solution networks, while others will be addressed by governments, the private sector or individual citizens. Initial proposals are outlined at the end of the report.

Prelude to a New Model of Global Governance

The Internet is now a worldwide phenomenon. In order to understand its multi-stakeholder model of governance, and the policy issues that have arisen due to its exploding global popularity, it's important to understand

Timeline of the development of the Internet[3]

how the Internet evolved.



The Original Vision

The Internet was designed initially in the late 1960s.[3] According to a paper titled "A Brief History of the Internet" published by the Internet Society,[4] the impetus for what became the Internet came from "a series of memos written by J.C.R. Licklider of MIT in August 1962 discussing his 'Galactic Network' concept. He envisioned a globally interconnected set of computers through which everyone could quickly access data and programs from any

site."[5] Licklider became head of the Defense Advanced Research Projects Agency (DARPA) and, according to the paper, "He convinced his successors at DARPA, Ivan Sutherland, Bob Taylor, and MIT researcher Lawrence G. Roberts, of the importance of this networking concept."[6]

Those designers were also working on the idea of packet switching and took Licklider's vision and, in 1967, created a networking concept under contract with DARPA that used information packets capable of taking different pathways through the network instead of requiring all the information to travel over the same pathway. The packets were then put back together in proper order when they were all received. In 1968, DARPA issued a contract to a company in Cambridge, MA, Bolt, Beranek and Newman, to develop a working model of the design, which was called an Interface Message Processor (IMP). The network that would be created by these interconnected IMPs was called the Advanced Research Projects Agency Network or ARPANET.

The first node of ARPANET was established at UCLA in 1969 and the second was set up at Stanford Research Institute (SRI) for the famous Augmentation of Human Intellect project run by Doug Engelbart, who is best known as the developer of the mouse and the concept of the Graphic User Interface (GUI), both of which dominate computing to this day. Two more nodes quickly followed at UC Santa Barbara and the University of Utah.

From ARPANET to Internet

ARPANET morphed into the Internet as it continued to grow and evolve technically. Robert Kahn and Vinton Cerf, who are often called the fathers of the Internet, developed the Internet's protocol, which was designed to carry packets over different media, including wire, radio systems and satellites. Their goal was to develop a robust protocol that was independent of both the content that was being carried and the type of network on which it was carried. Essentially, the protocol allowed communications between separate networks. While they called it Transmission Control Protocol (TCP), it contained components of the TCP/IP protocol now used on the Internet. The term Internet itself was first introduced in a paper published in December 1974 by Cerf, Yogen Dalal, and Carl Sunshine that described TCP's ability to foster internetworking.[7]

ARPANET grew significantly in the 1970s and early 1980s, moving from its original NCP protocol to TCP/IP in 1983. At that time, military computing split off from ARPANET, calling its network MILNET. ARPANET then consisted of 45 nodes, while MILNET had 68 nodes. MILNET was used for unclassified military communications, while academic researchers used ARPANET for non-military communications.[8]

Post-1983, ARPANET evolved as a network for academic research in a burgeoning technological world of commercial packet switching networks like Tymnet and Telenet, and a growing number of proprietary communications networks from the leading computer companies of the day, particularly IBM and Digital Equipment Corporation. ARPANET itself was

replaced over a five-year period from 1985 to 1990 by the NSFnet, which was a new backbone funded by the National Science Foundation (NSF) designed to interconnect a number of rapidly-developing regional TCP/IP-based networks that connected universities within each region.

This is a very important point that is often misunderstood about the Internet. TCP/IP was developed to allow a variety of different networks to be interconnected. When ARPANET was split from MILNET in 1983, it did not grow as a single network. Instead, universities across the country formed independent TCP/IP-based regional networks that were interconnected by the NSFnet, which was essentially a backbone network.[9] In the late 1980s, NSFnet kept adding independent networks from both the US government and academia, and also expanded internationally in North America, Europe and Asia.

Development of the World Wide web

As the Internet evolved in the 1980s, its two main applications were Simple Mail Transport Protocol (SMTP) to send electronic mail and File Transfer Protocol (FTP) to exchange computer files. In 1989, Tim Berners-Lee, a researcher at CERN in Switzerland, developed the World Wide web,[10] which he saw as a better way for academic researchers to communicate than either FTP or email. The web allowed papers to be published online and included the concept of hyperlinking so that you could jump from one paper directly to another. The concept was developed initially in the 1960s and had been used in several proprietary systems, but had not yet become mainstream.

Use of the web accelerated rapidly in 1993 when it was expanded to work with Common Gateway Interface (CGI), which allowed web pages to link to programs written in a scripting language, like Perl, and also to be integrated with databases. This allowed the development of ecommerce websites.[11]

Commercialization and the Birth of Policy Issues

As web and email applications opened up the Internet to new possibilities, one of the old ARPANET concepts started to come into question. Essentially, ARPANET was viewed as a non-commercial network for academic researchers. Thus, it was considered bad form to use it for any type of commercial activity. When ARPANET morphed into the NSFnet, non-commercialization became formalized in the NSF's Acceptable Use Policy that defined the types of traffic that could be carried over the NSFnet backbone.[12] Since the NSF itself was authorized by Congress to "foster and support the development and use of computer and other scientific and engineering methods and technologies, primarily for research and education in the sciences and engineering," it could only authorize the NSFnet backbone to carry traffic that supported those interests. Commercial use was forbidden.

In 1988, Vint Cerf, who was the co-developer of TCP/IP, convinced the Federal Networking Council, which coordinated communications policy among US government agencies, to allow a commercial email service,

MCI Mail, to interconnect to the Internet as an experiment. According to Cerf, several other commercial email services then asked to interconnect and quickly discovered that they could then exchange emails among their various customer bases because each network had to convert from their traffic to SMTP.[13]

Cerf's experiment was the precursor that led to the formation of several commercial ISPs, and as the need for commercialization became obvious, the Internet underwent another transformation. In 1992, Congress amended the NSF's charter so that commercial traffic could be carried over the NSFnet backbone.[14] Furthermore, the NSF transitioned out of controlling the backbone itself into providing a network used only by academic researchers. In essence, the Internet opened up its doors to commercial traffic.

The transition to carrying commercial traffic can be considered the Internet's first major policy issue. Before that transition, the Internet's issues had largely been technical in nature. Its developers were continually looking to refine how every layer of the Internet operated, and were doing it through what they termed working groups, which were set up to solve problems by collaborating among all the stakeholders.

All of a sudden, a policy issue was introduced that the Internet's developers could not solve technically: should commercial traffic be carried over the Internet and how could it be done within the NSF's charter? At the time, it was solved by the US Congress, which amended the NSFnet's charter and then transitioned the NSF out of providing the backbone so that its operation could be opened up to commercial telecommunications companies.

The Naming Gold Rush and Domain Names

One of the ARPANET's initial problems was that routing was done by numbers, while people using the network found names much easier to remember. So ARPANET's developers created the concept of using a text file, HOST.txt, to map these names to numbered addresses. When ARPANET's NCP protocol gave way to TCP/IP, the Domain Name System (DNS) was developed so that user organizations could create names that were then translated to numerical IP addresses using a distributed database structure that kept itself updated automatically via the network. In the 1980s, the DNS was something of a sleepy backwater. When the Internet had fewer than 100,000 users with only a few thousand organizations, DNS wasn't a big deal. In 1991, however, as the Internet was starting to grow, the US Defense Information Systems Agency subcontracted with Network Solutions, Inc., a small software firm in Washington, DC, to develop a more robust system. In 1992, Network Solutions was the sole bidder on grant from the NSF to develop the system further, including automated domain registration, and in 1993, it was given an exclusive contract for $5.9 million to be the Internet's sole registrar of domain names for the .com, .net, and .org domains.[15]

In 1995, the Internet started to grow explosively and the NSF gave permission for Network Solutions to charge for registering names. Up until that point, names could be registered at no cost. Nevertheless, since so few people

knew about the Internet and usage was non-commercial, only a relatively small number of names was registered. By 1995, however, the Internet had emerged from the shadows. About 20,000 new users were being added daily,[16] and thousands of businesses were setting up servers and planning to develop websites. Since Network Solutions made names available on a first-come, first-served basis, the naming gold rush was on. All that was needed to register a name was $100 for a two-year registration.

Domain Names and Intellectual Property Rights

As the Internet's growth accelerated, naming and intellectual property rights (IPR) became the Internet's second major policy issue, and the first one in which the Internet became intertwined with the legal system. Since anyone could register any name, enterprising entrepreneurs registered names that belonged to major businesses in hopes of reselling the names for a quick profit. This resulted in lawsuits and complaints about Network Solutions' naming policy. The resulting lawsuits were complex because the courts hadn't dealt with an issue of this kind, and new legal precedents were being established.

In 1999, the US Congress passed the Anti-cybersquatting Consumer Protection Act, which clarified rights that people or business organizations had over their own or similar names and their valid trademarks.[17] While the Act hasn't resolved all lawsuits, it has at least clarified the law for the courts when lawsuits are filed.

Domain name registrars now operate under a Uniform Domain Name Dispute Resolution Policy, put in place by the Internet Corporation for Assigned Names and Numbers (ICANN), which is designed to protect against abusive registrations. When a domain name is registered, the registrant asserts, among other things, that the name will not infringe upon or otherwise violate the rights of any third party. If there is a dispute, the third party is then required by the registrar to prove each of three points:[18]

1. The domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights.
2. Registrant has no rights or legitimate interests with respect to the domain name.
3. The domain name has been registered and is being used in bad faith.

An administrative proceeding on the dispute would follow,[19] and a decision made on cancellation or transfer of the domain name.

"When the Internet emerged into the mainstream as a commercially-oriented network, a raft of policy issues that had not existed before came to the forefront adding a new dimension: a tangle of legal issues on an international scale."

The New World of Policy Issues

As Internet growth accelerated in the 1990s, a distinct gap developed between so-called technical and policy issues. The Internet developed as it did because its developers had a long history of working together in a collaborative manner to solve technical or operational problems, against core principles of *inter alia* openness and de-centralization, as enablers of free choice. At the time, it is doubtful that there was a consciousness of "Internet governance" and those involved in developing and operating key parts of the Internet's infrastructure certainly did not use the term.

When the Internet emerged into the mainstream as a commercially-oriented network, a raft of policy issues that had not existed before came to the forefront adding a new dimension: a tangle of legal issues on an international scale. When Tim Berners-Lee named the World Wide web, he envisioned a spider web of interconnecting websites. He got the spider web he envisioned, but he also got a spider web of legal systems and jurisdictions worldwide, each of which reacted to issues that were mushrooming because of online usage, poorly understood key elements of how the Internet actually worked, and the conflation factors mentioned above.

Consciousness of Internet Governance Emerges

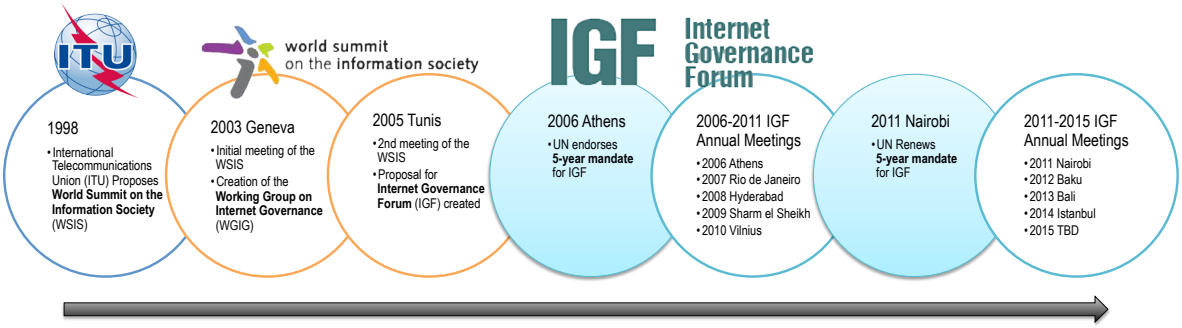
As the Internet was spreading worldwide, leaders in numerous countries began asking about who ran the Internet and how was it "managed." In particular, a lot of attention was focused on naming and addressing because of the importance of obtaining IP addresses for users within each country and of obtaining domain names for websites.

In the first part of this milennium, the UN General Assembly endorsed a proposal to hold the World Summit on the Information Society (WSIS).[20] It was held in two parts with two UN Summits and multiple preparatory sessions. Going into the first summit, WSIS I, held in Geneva in 2003, the WSIS was focused on building a foundation for "an Information Society for all," and addressing what was seen as a growing digital divide between industrialized and developing nations. One of the major issues that arose: who should govern the Internet?

As a result of WSIS I, the UN established the Working Group on Internet Governance (WGIG) to explore governance issues. In June 2005, WGIG released a report on its recommendations for Internet governance to aid in negotiations at the second summit, WSIS II, which was held in Tunis in November 2005.

The report had a number of proposals, but only two were supported in the *Tunis Agenda for the Information Society*, the final documents from WSIS II.[21] The supported proposals were the definition of Internet Governance, and the creation of an Internet Governance Forum (IGF).

Internet Governance Forum: Creation and Development Timeline



What Is Internet Governance?

While the WGIG's report might be considered the birth of the concept of Internet governance, the reality is that Internet governance began back in the 1970s as the Internet was evolving. The Internet's founders worked from the principle of an open Internet that would be operated using a multi-stakeholder model based upon meritocracy, collaboration and consensus and evolve based on needs. All the organizations playing a role in Internet governance today were built on needs and with community support and resources, and were not created from a top down hierarchical or centralized model.

Nevertheless, the Internet has become the world's communications system and some in the United Nations have been focused on its governance for more than a decade. Some support its model of continual multi-stakeholder evolution and some support additional oversight from the UN. Governance, which was at one time an unspoken concept within the Internet community, is now a recognized topic. What was once something that was practiced without a name has now become an important concept that is debated in numerous conferences and corridors of power worldwide.

What, then, is Internet governance? From a practical standpoint, the core leadership of Internet governance remains within the institutions established in the 1990s and earlier, including the Internet Society, the Internet Engineering Task Force, Internet Architecture Board, Regional Internet Registries (RIRs), TLD's and ICANN. These organizations all have open, inclusive processes. Each of the Internet organizations (the so-called I* orgs.) engages quite robustly with governments, civil society, individuals and the private sector, and these engagements differ by organization or issue.

In any discussion on Internet Governance, we have to consider various roles currently undertaken by the US Commerce Department's National Telecommunications and Information Administration (NTIA), or by ICANN under contract with NTIA. The NTIA's historic announcement in mid-March 2014 underlines the US government's confidence in the multi-stakeholder model. The announcement said:

To support and enhance the multi-stakeholder model of Internet policymaking and governance, the US Commerce Department's National Telecommunications and Information Administration (NTIA) today announces its intent to transition key Internet domain name functions to the global multi-stakeholder community.

The Tunis Agenda goes on to state:

Article 35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

a. *Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.*

b. *The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.*

c. *Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role.*

d. *Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.*

e. *International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.*

It's important to note that as a first step the NTIA is asking ICANN to convene global stakeholders to develop a proposal to transition the current role played by NTIA in the coordination of the Internet's domain name system (DNS).

"The timing is right to start the transition process," said Assistant Secretary of Commerce for Communications and Information, Lawrence E. Strickling. "We look forward to ICANN convening stakeholders across the global Internet community to craft an appropriate transition plan." Some implications of this announcement are covered later in this paper.

From a broader standpoint, Internet governance also includes the mushrooming industry associated with thinking about Internet governance and making proposals to alter its actual governance. As an example, the formal documents from the second (and final) phase of the UN WSIS

> *"Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."*

Summit—called the *Tunis Agenda for the Information Society*—included a working definition of Internet governance as follows:

> *Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*

The working definition is important because it doesn't just encompass the technical issues that shape the Internet, but the shared principles, norms, rules, decision-making procedures and programs as well.

The Tunis Agenda also stated that the WGIG report "enhanced our understanding of the respective roles and responsibilities of governments, intergovernmental and international organizations and other forums as well as the private sector and civil society from both developing and developed countries."

In short, the Tunis Agenda gives us a very good roadmap for the continual evolution of the multi-stakeholder Internet governance model, and provides clear guidance on how to address current and future policy issues.

A Taxonomy of Internet Issues

As the Internet has evolved, so too have numerous issues associated with its usage. These issues can be incorporated into a taxonomy as follows:

- People-to-People Interaction
- People-to-Business Interaction
- Organized Criminal Activity
- Privacy and Security
- Internet Business Practices

People-to-People Interaction

As social interaction on the Internet has exploded globally, so have issues associated with those interactions. Many of these issues are covered by existing societal laws and norms, such as slander and libel, but there have been a few that have required new norms or in some cases new laws.

The tragic case of Megan Meier[22] illustrates one of the problems. Meier committed suicide in 2006 a month before her 14th birthday because she developed a close online friendship with a Josh Evans. As the friendship grew deeper, Evans' tone changed from boyfriend to critic, most seriously when he wrote to her in a communication, "Everybody in O'Fallon [the town where she lived] knows who you are. You are a bad person and everybody hates

you. Have a shitty rest of your life. The world would be a better place without you." Meier hanged herself later that night.

The Meier story exploded into international news when it was uncovered that Josh Evans did not exist. He was created by Lori Drew, the mother of one of Megan's classmates. Drew felt that Megan was spreading gossip about her own daughter, so she created the fake profile to teach Megan a lesson. The Megan Meier story reverberated worldwide. As a result of the Meier and other troubling incidents that have taken place online, legal jurisdictions worldwide have adopted laws associated with impersonation and cyberbullying.

The bottom line in this area is that issues stemming from people interacting will continue to arise. Most will be handled within existing laws, but there will occasionally be issues that require more action whether through social norms or regulation.

People-to-Business Interaction

The Internet has opened the door to entirely new relationships between people on the Net and a wide variety of businesses. While most of these interactions are covered under existing societal laws, the nature of the Internet has changed the nature of the interactions in a fundamental manner, giving rise to a few major and complex concerns. Examples are intellectual property rights (IPR) and privacy.

Protecting IPR predates the Internet by 100 years. The 1886 Berne Convention protected copyrighted works by treaty in multiple countries.[23] Over the years, the treaty was revised eight times. At present, 165 countries are party to the Convention.

The Internet obviously accelerates issues associated with protecting IPR because of the speed and facility with which information can be published and spread worldwide. In fact, IPR was one of the first global issues as individuals reserved domain names and then tried to sell them to interested parties. While this forged new areas of law in the early days of the commercial Internet, it has now evolved into a reasonably well-defined area in which copyright and trademarked names are properly protected.

Copyright became an even bigger issue as peer-to-peer networks allowed people to share things like songs and videos. While copyright owners have fought successful battles against such networks as Napster, evolving IPR remains one of the biggest and most complicated issues, spanning policy, technical, cultural and commercial considerations.

The Internet opens up the opportunity for a radical rethink about IPR. In the traditional model, IPR was something to be kept private and under control. In the new model enabled by the Internet, sharing information and IP can often lead to unexpected opportunities. This is an evolving topic that is covered in detail in Don Tapscott's and Anthony Williams' books *Wikinomics*[24] and *MacroWikinomics.*[25]

Organized Criminal Activity

The Internet has proven to be fertile ground for organized criminal activity.

Spam

In the world of electronic mail, "entrepreneurs" flood mailboxes with unsolicited commercial pitches—a variety of email "spam."[26] While spam may be no more than a nuisance to many users and is clearly not a crime just because unsolicited emails are sent, spammers often cross the line by hacking into existing email systems and stealing not just the names of system users, but also their contact lists. The result: an explosion in uninvited commercial solicitations. While the emails themselves are not illegal, the hacking and theft of names certainly is.

In short, spam has evolved into an international policy issue for the governance network and was one of the issue at the World Conference on International Telecommunications 2012 (WCIT-12) in Dubai. Article 7 of the International Telecommunications regulations (ITRs) developed at the conference said, "Member States should endeavor to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services."[27]

Since everyone hates spam, it sounds like Article 7 of the ITRs should be noncontroversial. However, the US opposed it because, said US delegation leader Terry Kramer in a press conference,[28] it "opens the door to regulation of other forms of content, including political and cultural speech."[29] In short, as hated as spam might be, it is tied directly to the issue of free speech and illustrates the two fundamental problems associated with almost any Internet-related policy issue. First, different countries can easily have different opinions about how to handle the issue within their systems of laws. And second, even if one country has a law prohibiting a form of Internet communication, how is it enforced when communication originates in another country and flows over the network to people across geographic boundaries?

The spam problem is particularly egregious in developing countries where it can overwhelm capacity and divert resources, becoming a crippling economic burden. This consideration makes spam a priority. Otherwise, spam can largely be addressed through a combination of technical, operational and policy means—and hence is not seen by most as requiring centralized Internet governance mechanisms or oversight, but rather better mechanisms for sharing solutions.

Credit Card Fraud and Identity Theft

The rapid development of ecommerce has given rise to two new policy issues: credit card fraud and identity theft. Neither of these issues is new, of course, but the Internet has added to their complexity on a global scale. Before online services, a criminal had to find "identity numbers" physically in order to steal an identity. With the advent of the Internet, criminals can now "phish" for names and identity numbers online and then construct fake identities that use those names and numbers in a random, impersonal way.

The same is true with credit cards. Criminals can phish to find credit card numbers online and then sell them for quick use before the individuals and credit card companies can react. Credit card fraud, furthermore, has an even more alarming dimension. Because of the massive growth in online shopping, there are numerous companies who take credit cards and store them in their online databases. Criminals are continually developing techniques to hack into databases of financial and personal information for fraudulent purposes.

Pornography and Protecting Children

While we often want to ignore it, so-called adult entertainment is a money-maker on the Internet. The problem comes when adult entertainment crosses the line into pornography and even child prostitution. One issue is preventing non-adults from accessing the information; a second is jurisdictional. How can laws be created and action taken against websites operating across juristictional boundaries? Internet pornography has also evolved into a more serious dimension: cybersex trafficking. CNN, for example, recently told the story of a 14-year-old Filipino from the rural countryside who was lured into a major city by a cousin. Instead of getting babysitting work, she was forced to perform sex acts with other young girls in order to satisfy the fantasies of men watching them by video over the Internet.[30] In the article, the CNN reporter wrote:

> *Alforque, Advocacy Officer with End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (ECPAT Philippines), an NGO working to combat child sexual exploitation, explained that because cyber-sex dens can be located anywhere—from Internet cafes to private homes and offices—they are extremely difficult to identify. Anyone who has a computer, Internet and a web cam can be in business.*
>
> *Whether part of large international criminal syndicates or smaller operations, their independent nature and lack of coordinated structure make it easy for cyber-sex operations to remain hidden, she said.*
>
> *According to Andrey Sawchenko, National Director at the International Justice Mission Philippines, the private nature of the technology allows the crime to take place in a venue that law enforcement can't easily access—and that makes it harder to gather evidence against perpetrators.*

Ironically, the most hope one has for stopping this kind of trafficking is the ability to track activity over the Internet—following due process, of course. While such cybersex dens might be hard to identify, once they are, it's not particularly difficult to find out where the den is located and to also identify all of their users.

Privacy and Security

With the recent revelations of mass surveillance, privacy has emerged as the most significant issue associated with Internet usage. The ultimate goal should be privacy *and* security, and there are efforts underway, notably at the Internet Engineering Task Force, to move the world closer to this goal. In the meantime, key privacy issues include:

- What control do users have over the use of information they place on social networks?
- Are governments (Big Brother) watching what we do on the Internet and how can this be controlled better by users?
- Are corporations (Little Brother) tracking and using too much data on not just what we purchase, but what we look at on the Internet or on our traffic patterns in physical marketplaces?
- Are the users (Baby Brother) creating their own problem by disseminating personal information without adequate regard for its ultimate use?

Perhaps the most basic privacy issue is: What control do we have over the personal information that we place on the Internet or that can now be collected using such technology as facial recognition? Do we own our information, or is it owned by the application developer or service provider? Can prospective employers, or colleges we apply to for admission, require us to show them information we reveal on social networking sites? Can our friends copy and disseminate the information we put on the Internet without our permission? What rights do we have about the information collected through ecommerce transactions? The list of questions goes on and on, and the only way to answer them is through the laws of the societies in which we live, which gives rise to a web of differing rulings and interpretations.

Interestingly, the Terms of Service (TOS), also known as Terms and Conditions, published by major companies like Facebook, Google or Amazon.com are legal contracts that have become the *de facto* documents controlling users' privacy, which is its own issue. Should Internet companies be allowed to set their own terms and conditions or should there be some set of legislated requirements that govern?

Big Brother

Concern about government spying on citizens exploded into international prominence when Edward Snowden disclosed that the US government was collecting records of Internet traffic as part of its anti-terrorism efforts.[31] This aspect of privacy is closely related to the issue of government jurisdiction over the Internet. The most important thing to understand is that you leave a trace (a "digital footprint") of your activities on the Internet every time you go online. This happens through cookies that are left on your computer and through websites capturing your IP address every time you visit. Governments are able to watch what its citizens are doing on the

Internet, and Internet service providers can assemble a sizable dossier on what a specific computer is doing as well. The conditions under which this is allowable has become a major issue, especially with the revelation that the US government has programs—PRISM and XKeyScore—that collect and store Internet communications from millions of its citizens[32] and has also broken the encryption scheme that is commonly used for financial transactions and to send supposedly secure information.[33]

Little Brother

Privacy advocates have dubbed corporations Little Brother. The items we purchase over the Internet and the advertisements we look at constitute another privacy issue. Businesses big and small are watching what we do on the Internet and customizing how they interact with us as a result. This is done through massive back end databases that keep track of what we buy and what ads we click on. It's not an accident that when you click on an ad or even visit a web page, you'll start seeing ads related to that activity on other web pages you visit. In essence, the many commercial companies now on the Internet are tracking your behavior and tailoring ads to map to that behavior. They also get your permission from the terms of service that are on their websites. When you use their websites, you often and perhaps unknowingly agree to allow them to track you through the "cookies" they set.

Now for the big question: are corporate promotional actions good or bad? Many people think it enriches their Internet experience to have companies tailor advertising and make suggestions about things they might be interested in based on past behavior. Many others don't care either way. Still others, however, think that it is problematic or perhaps unsettling to have such a record of activity tracked regularly, especially if governments could assemble that information to create a dossier of Internet usage on any individual.

Baby Brother

There is a new kid on the block. As cartoonist Walt Kelly once said in his famous Pogo cartoon strip, "We have met the enemy, and he is us."[34] Hundreds of millions of people are revealing detailed data about themselves, their activities, their likes/dislikes, etc. online every day. This situation has turned traditional privacy laws and regulations upside down. Privacy and data protection laws emphasize the responsibility of organizations to collect, use, retain and disclose personal information in a confidential manner. Collaborative networks, in contrast, encourage individuals themselves to directly and voluntarily publish granular data, short-circuiting the obligations of organizations to seek informed consent.

Most users don't think about understanding the privacy settings on their browsers and don't use available privacy settings on social sites, thereby allowing a massive amount of data about themselves to flow onto the Internet. Nevertheless, our unwitting practice of what might be termed radical openness is arguably a big mistake. Personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, is the stuff that makes

> *"The first Internet boom…resembled a religious movement. Omnipresent cyber-gurus, often framed by colourful PowerPoint presentations reminiscent of stained glass, prophesied a digital paradise in which not only would commerce be frictionless and growth exponential, but democracy would be direct and the nation-state would no longer exist."*

up our modern identity and is the foundation of our personal security. It must be managed responsibly—and not just by others, but by each of us. Each of us needs a personal privacy strategy governing what information we release to whom, and rather than default to openness, we should consider defaulting to privacy and then choosing where and with whom to share information.

For more on the importance of protecting personal privacy, see Don Tapscott's seven-part series in *The Huffington Post*. Part one is titled, "Should We All Be More Open."[35]

The bottom line is that all of these privacy issues have opened up a massive can of worms. It is no longer just the Orwellian model of Big Brother watching us, although revelations like the XKeyScore program make that more concerning than ever. Little Brother is also keeping track of everywhere we go on the Internet and many of the things we buy, so that it can maximize the efficiency of the Net's ecommerce engine. Finally, apathy may be the most concerning as Internet users don't seem too troubled about the increasing lack of privacy or indeed the increase in pervasive surveillance being practiced by many governments across the world.

Government Jurisdiction

The Internet from its very beginning has been based upon openness and freedom of speech. Nevertheless, not every government in the world has the same view on what it means to have such freedom. As such, different governments have developed significantly differing views on what their citizens should see or access on the Internet.

Many observers are concerned that the Internet may be "balkanized," meaning that different countries will compromise the Internet's openness through powerful filters that limit what its citizens can see. There is also concern that Internet Service Providers might start charging different rates for access to different types of content on the Internet, thereby creating information tiers.

In September of 2010, The Economist published an article titled "A Virtual Counter-revolution" in which it wrote:[36]

> *The first Internet boom, a decade and a half ago, resembled a religious movement. Omnipresent cyber-gurus, often framed by colourful PowerPoint presentations reminiscent of stained glass, prophesied a digital paradise in which not only would commerce be frictionless and growth exponential, but democracy would be direct and the nation-state would no longer exist. One, John-Perry Barlow, even penned "A Declaration of the Independence of Cyberspace"…*
>
> *Fifteen years after its first manifestation as a global, unifying network, it has entered its second phase: it appears to be balkanising, torn apart by three separate, but related forces.*
>
> *First, governments are increasingly reasserting their sovereignty … Second, big IT companies are building their own digital territories, where they set the rules and control or limit connections to other parts of the Internet. Third, network owners would like to treat different types of traffic differently, in effect creating faster and slower lanes on the Internet.*
>
> *It is still too early to say that the Internet has fragmented into "Internets", but there is a danger that it may splinter along geographical and commercial boundaries…*
>
> *The Internet is too important for governments to ignore. They are increasingly finding ways to enforce their laws in the digital realm. The most prominent is China's "great firewall". The Chinese authorities are using the same technology that companies use to stop employees accessing particular websites and online services…*
>
> *But China is by no means the only country erecting borders in cyberspace. The Australian government plans to build a firewall to block material showing the sexual abuse of children and other criminal or offensive content. The OpenNet Initiative, an advocacy group, lists more than a dozen countries that block Internet content for political, social and security reasons.*

The OpenNet Initiative mentioned in the article keeps track of how each country handles Internet filtering and publishes global maps based on four different criteria: political, social, conflict/security and Internet tools.[37]

> *"The Internet has numerous challenges...that typically do not have "solutions" in the technical sense and can't be solved with hardware/software protocols. These issues involve human behavior, cultural differences, political ideology, economic considerations..."*

Far from fading away, the issues associated with government jurisdiction and net neutrality will likely become the most important during the next decade. The governments who lost the battle at WCIT 2012 in Dubai[38] have certainly not lost the war, at least from their perspective. They are all actively implementing ways to control what their citizens can access on the Internet and looking at technologies that can improve the process.

Business Practices of the Internet Industry

The major issue at the moment associated with Internet business practices falls under the rubric of net neutrality, which is "the principle that Internet service providers and governments should treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, and modes of communication."[39]

Tim Berners-Lee, who is one of the Internet's leading proponents of net neutrality, says that it is about the web being an open market, so anybody can participate. "There should be no commercial bias, no political bias in the delivery of the packets," he says. "That's what neutrality is about."

Net neutrality, however, is under fire from Internet Service Providers. In the US, for example, a federal appeals court recently ruled that the Federal Communications Commission overstepped its bounds by trying to impose a net neutrality rule on domestic ISPs on the technical grounds that the FCC lacks jurisdiction to regulate the Internet.[40] The ruling, unless overturned by the US Supreme Court, basically requires that Congress pass net neutrality requirements on ISPs, otherwise they will be free to establish different charges for different types of traffic.

Net neutrality is not based upon charging a flat monthly rate for unlimited Internet usage. It is based upon the idea of not distinguishing between bits that flow over the Internet. Many ISPs, for example, charge based on the amount of data that an Internet user consumes, which many people might consider fair, but they do not distinguish between the various types of data, such as a video, a voice call, a blog post, an email, etc. This type of neutrality would likely be threatened if the Internet were transferred to the ITU.

Addressing the Policy Challenges Facing the Internet Governance Network

The Internet has numerous challenges, including technical, operational and what might be termed "big P" policy issues—those that typically do not have

"solutions" in the technical sense and can't be solved with hardware/software protocols. These issues involve human behavior, cultural differences, political ideology, economic considerations, etc. Resolving them requires a range of issue-focused stakeholders, often on a global level.

Different Set of Stakeholders

In order for an Internet governance network to function properly, it needs the right set of stakeholders participating—at the opportune time. Generally speaking, the Internet ecosystem has the right stakeholders to handle its technical and operational issues, but it needs broader engagement in order to best handle the "big P" policy issues. Potential stakeholders in this realm are often to be found within the web of legal jurisdictions at local, state, national and international levels. Many current stakeholders are associated with the private sector, governments or the UN, or are trying to work through UN or intergovernmental processes occasionally adapted to fit multi-stakeholder expectations. And, many of those processes are found wanting as they do not provide adequately for all necessary voices. The UN has had an increasingly difficult time resolving global issues like climate change, fighting poverty or achieving the Millennium Goals. How can we expect these stakeholders to resolve Internet usage problems based on their present track record?

Can the "Big P" Policy Issues be Addressed Adequately?

Can these "big P" policy issues be resolved? Will we ever be able to break through the continual escalation inherent in some of these areas? Should we even expect to? These issues are complicated whether because of conflicting goals and jurisdictions, or the pace of change vs. pace of policy-making processes. Internet criminals, for example, try to set up in jurisdictions worldwide that do not have extradition treaties with the main countries in which they are generating their revenues. Thus, even if laws are passed and the criminals are identified, there's not much that the prosecuting country can do to bring them to justice without equivalent laws and cooperation from the jurisdiction where the criminals are located. Blocking their domains and IP addresses doesn't help. They just set up new domains and change their IP addresses. Many of these cybercriminals operate outside the reach of the law, making it hard for anyone to resolve the problems.

Nevertheless, that doesn't mean that major progress can't be made on many of these issues or that the Internet governance network is not up to the task. The problem isn't particular to the Internet either, but typically is related to issues of sovereignty and jurisdiction that have perplexed governments for years. As ISOC likes to point out, solutions require dialogue and openness, so part of its charter is to bring relevant parties together to work toward the

best solutions, and it has successfully worked on quite a number of global Internet governance issues. To cite just one example, ISOC has played a significant role in working with various key IPR stakeholders like the World Intellectual Property Organization (WIPO), the Organization for Cooperation and Development (OECD) and various large content providers, industry associations and users to help them work together to better understand and address this complex area.

To this end, Nitin Desai, who headed the UN's Working Group on Internet Governance (WGIG) and has played a major role in the evolution of the Internet Governance Forum (IGF), has developed a model called Fuzzy Law which has promise to make headway in the "big P" policy arena. Instead of debating issues to the point where countries worldwide adopt a single law, Fuzzy Law allows for what Desai terms "a margin of national interpretation." Instead of countries adopting a single law, they would try to reach broad consensus on key policy issues and then draft laws to fit within each country.

"You need to look for something that isn't as definite at the international level as you would find at the national level," he says. "There need to be margins of interpretations within the different countries. We must focus more on things that require cooperation between countries….If we go for fuzzy law as distinct from hard law, it is possible to make a lot of headway. The UN's human rights achievements never would have evolved if we insisted that every country follow precisely the same detailed provisions on the protection of rights….Basically, you have to allow for margins of interpretation and not insist that everybody has to do it exactly the same way."[41]

Implications for Network Leaders

The Internet's multi-stakeholder governance ecosystem has evolved over the years in response to identified needs, and does its job in a highly complex environment that involves a global network of stakeholders with diverse and not always compatible interests. As the Internet continues on its path to encompass the globe's 7+ billion citizens, its governance will face increased scrutiny and numerous challenges in charting a course that keeps the Internet free, open and able to fulfill it's potential for prosperity and social development.

While the Internet governance network may be here to stay, that doesn't mean that it will be static. There are now numerous activities or studies underway worldwide about what should happen to Internet governance. Here is a sampling:

- In February 2014, the Panel on Global Internet Cooperation and Governance Mechanisms met in Rancho Mirage, CA, as part of a series of meetings to discuss the future of Internet governance. The panel consists of a number of influential stakeholders who plan to publish a high-level report on how Internet Governance should evolve.
- In April 2014, Brazil is hosting The Global Multistakeholder Meeting on the Future of Internet Governance. It will focus on crafting Internet governance principles and proposing a roadmap for the further evolution of the governance ecosystem. The meeting follows an initiative proposed by CGI.br and /1net.[42] Interestingly, it is co-chaired by individuals from the technical community, private sector, civil society and academia.
- The IGF will hold its annual meeting in Istanbul in September 2014, with the second round of preliminary MAG meetings taking place in Paris in May. The IGF has been and will likely continue to be one of the key forums for global governance.
- The ITU Plenipotentiary conference to elect officers and create a 4-year strategic plan for the Union will be held in Butan, Korea, in October and November of 2014. Following the eventful WCIT meeting in Dubai in 2012, Internet governance is expected to be a significant topic of discussion.
- The European Union presently has an initiative to study Europe's role in Internet governance and has placed an open call for papers soliciting opinions.
- Numerous consulting organizations are conducting Internet governance studies as the issue continues to emerge.

Internet governance continues to be a hot topic being discussed by numerous governments, the United Nations and within the ecosystem itself.

Evolution, Not Revolution

While the topic may be hot, especially with many people and governments outraged about the revelations that the US government (and many other governments around the world) supports mass surveillance programs, it is highly unlikely that there will be any significant or hasty changes to the Internet governance network. Janis Karklins, Assistant Director of UNESCO,

President of the Preparatory Committee for the 2nd phase of the United Nations World Summit on the Information Society (WSIS), and a former member of ICANN's board of directors as Chair of the Governmental Advisory Committee (GAC), said that the Internet was now far too important to the world economy to expect any rapid changes to its governance.

"There will not be a revolution," Karklins says. "It will be an evolution in any circumstance because there is too much at stake. The Internet as a technology is the underlying feature of modern economies and I think no one is really interested in breaking the system. Nevertheless, there are a number of concerns, these concerns are legitimate and we need to address them in an orderly manner."

The key conclusions and implications for leaders of the diverse organizations and individuals that currently participate or aspire to participate in the Internet governance network follow.

Continue to Engage the Developing World

One of the continuing Internet governance issues is the so-called North/South, or digital divide. Industrialized countries are criticized for not doing enough to properly engage the developing world. With 5 billion of the world's population still to come online it will be broadly beneficial to ensure full participation from the developing world in all Internet governance matters.

While an Internet governance network alone can't resolve the digital divide, greater participation in this ecosystem could help solve many of the development and economic problems the "South" countries face, and will also add to the legitimacy of the ecosystem itself. To this end, it appears that the Internet governance network is poised to receive help from companies like Google and Facebook, which have launched major initiatives to continue the spread of the Internet to developing economies globally, taking a major bite out of the digital divide.

Take the Threat to Move Internet Control to the United Nations Seriously

The Showdown at Dubai was basically a move to have the UN, through its International Telecommunications Union (ITU), take more control of the Internet. As Janis Karklins says, "We have made significant progress in accepting a multi-stakeholder model of Internet governance since 2004 but… we are not there yet. The push for an intergovernmental model of Internet governance where governments would be fully in charge is again gaining ground."

Interestingly, the threat from the ITU or any other intergovernmental agency to take control over Internet governance is closely related to how well the Internet governance network can engage the developing world.

At the moment, the threat is fairly small because the US government and its allies have been very successful in blocking any such attempts. The US government, for example, would not be considering ending its contract with ICANN if it felt that this would lead to the governance of the Internet being taken over by the ITU. Nevertheless, this is likely to be an on-going concern.

If the ecosystem is successful in finding better ways for the developing world to participate in Internet governance, this will likely go a long way toward ending the threat.

Watch For the Development of an Internet "Magna Carta"

Tim Berners-Lee recently used the 25th anniversary of the World Wide Web to call for "the web we want" initiative. As part of the initiative, Berners-Lee called for the development of a "Magna Carta," which would be "a global constitution—a bill of rights" that would protect people using the Internet. According to an article in the Guardian, Berners-Lee said that "the web had come under increasing attack from governments and corporate influence and that new rules were needed to protect the 'open, neutral' system."[43]

Fittingly, instead of pushing to have this Magna Carta developed within government, Berners-Lee has called for interested Internet users inside every country to generate versions of a digital bill of rights that can be widely supported within each country.

In the Guardian article, Berners-Lee says, "Unless we have an open, neutral internet we can rely on without worrying about what's happening at the back door, we can't have open government, good democracy, good healthcare, connected communities and diversity of culture. It's not naive to think we can have that, but it is naive to think we can just sit back and get it."[44]

Since "the web we want" initiative is new, it's not clear whether it will gain any traction among web users. Nevertheless, it is an interesting idea because it is calling on web users in each country to come together to develop a digital bill of rights. If it gains traction, the Internet Governance Network will undoubtedly have to take notice.

Expand the Development of Internet Exchange Points (IXPs)

One issue that will become increasingly important, perhaps even critical, is how information flows over the Internet. At present, a number of developing countries have information pathways that flow through the IXP (Internet Exchange Point) backbones in industrialized countries in order to move information not just between other countries that may be closer geographically, but even between Internet service providers (ISPs) within their own countries. Brazil, for example, is already starting to develop fiber optic cable links to Western Europe and Asia in order to eliminate information flowing through US backbones, while Mexico is largely dependent upon backbones in the US to move its traffic between ISPs within its own country.

One of the growing calls worldwide will be for information to be retained within each country until it needs to flow to other countries in order for these countries to control their own data security. In practice, this will mean establishing IXPs within each country to control the flow of information between their internal ISPs and to IXPs in other countries. While the number of IXPs in the world has been growing rapidly, and now numbers about 300, there are still something like 88 countries worldwide that do not have an IXP.[45]

Support the Transition of Key Internet Domain Name Functions

In mid-March 2014, the US Commerce Department's National Telecommunications and Information Administration (NTIA) announced its "intent to transition key Internet domain name functions to the global multi-stakeholder community."[46] During the past year, in particular, there have been increased calls for the US government to make such a transition. Tim Berners-Lee, for example, recently said, "The removal of the explicit link to the US department of commerce is long overdue. The US can't have a global place in the running of something which is so non-national. There is huge momentum towards that uncoupling but it is right that we keep a multi-stakeholder approach, and one where governments and companies are both kept at arm's length."

Fadi Chehadé, the CEO of ICANN, reflects the enthusiasm of the ecosystem, saying, "To me this was more than a good decision, it was a most courageous and gracious action." He says that as an immigrant, the decision gives him pride and hope as this is a validation of the American spirit. "We invent something wonderful and then we give it to everyone," he says.

While the US decision was met with accolades within the Internet governance network, a counter-reaction has developed swiftly within conservative US political circles. For example, former Bush administration State Department Senior Advisor Christian Whiton was quoted in a small news website, *The Daily Caller,* as saying, "This is the Obama equivalent of Carter's decision to give away the Panama Canal—only with possibly much worse consequences. While the Obama administration says it is merely removing federal oversight of a non-profit, we should assume ICANN would end up as part of the United Nations. If the UN gains control over what amounts to the directory and traffic signals of the Internet, it can impose whatever taxes it likes. It likely would start with a tax on registering domains and expand from there."[47]

From our perspective, this is an over-reaction that is likely to be resolved by a better understanding of the Internet governance network, whose many organizations have been managing these key functions responsibly for many decades.

Returning to the recent NTIA announcement: "NTIA's responsibility includes the procedural role of administering changes to the authoritative root zone file—the database containing the lists of names and addresses of all top-level domains—as well as serving as the historic steward of the DNS. NTIA currently contracts with ICANN to carry out the Internet Assigned Numbers

Authority (IANA) functions and has a Cooperative Agreement with Verisign under which it performs related root zone management functions."[48]

The IANA contract covers three Internet registries: the protocol parameter registry, the domain name registry (which essentially has the root zone in it) and the Internet Protocol (IP) address registry.

It is important to understand that the IANA functions operated by ICANN are in fact managed under various agreements or processes with the organizations mentioned below. The policies and oversight for these registries are established through open community processes under the leadership of the following bodies: Protocol Parameters in the Internet Engineering Task Force (IETF), IP Addresses in the Regional Internet Registries (RIR's), and Domain Names in ICANN. This last point is not well understood and has led to confusion for many on ICANN's role. It has also led to understating the roles played by other Internet organizations.

All the Internet organizations (I* orgs.) have been active, particularly over the last three to four years, in reviewing and documenting how the key Internet domain name functions are managed. Convened by the Internet Society (ISOC), the I* organizations are working together to document how these "Shared Internet Resources" are being managed. As ISOC says: "The smooth operation of the Internet depends upon a global, coordinated, community-driven approach to managing these key shared resources."[49] It also breaks out separate roles for each of the registries: Protocol parameters, IP addresses and Domain Names. For a more in-depth and technical read, see the Internet Architecture Board document titled, "A Framework for the Evolution of the Internet Assigned Numbers Authority (IANA)."[50]

The NTIA announcement means that it no longer expects to administer the root zone management function and also no longer plans to have stewardship of ICANN. The NTIA, however, said that any transition needs to assure that the root zone management and registry functions are properly performed. "One of the genius moves of the NTIA announcement," says Fadi Chehadé, "is that they did not prescribe what is that mechanism, they simply said we are such believers in the multi-stakeholder model that we're going to let it come up with the right mechanism. We believe in it. We trust it. We trust that ICANN can run that process openly and with accountability."

This is an extremely important point. The US government is not "giving away the Internet," as has been claimed by a number of pundits. Instead, it is completing the process of privatization of the DNS as outlined by the US government in 1997 and within the multistakeholder model it has always supported.

Instead of giving away the Internet, the US government is completing the creation of a juggernaut that has spread worldwide because of its open, distributed, adaptable platform and its supportive multi-stakeholder governance network.

The NTIA, however, is not just declining to renew the contracts. It expects that ICANN will develop a proposal for an acceptable mechanism "collaboratively with…the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Society (ISOC), the Regional Internet Registries (RIRs), top level domain name operators, VeriSign, and other interested global stakeholders," according to its recent press release.[51]

Unless ICANN can develop a proposal that has broad community support and meets the following criteria, the NTIA has said it will not accept it:

- Support and enhance the multi-stakeholder model
- Maintain the security, stability, and resiliency of the Internet DNS
- Meet the needs and expectation of the global customers and partners of the IANA services and,
- Maintain the openness of the Internet.

Furthermore, the NTIA said, "Consistent with the clear policy expressed in bipartisan resolutions of the US Senate and House of Representatives (S.Con. Res.50 and H.Con.Res.127), which affirmed the United States support for the multi-stakeholder model of Internet governance, NTIA will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution."

Fadi Chehadé said that he believes the mechanisms are largely in place to satisfy the NTIA's requirement. He said that the IETF creates the policies in the protocol parameters registry and that the Internet Architecture Board (IAB) meets four times a year with ICANN to review how it's administered and implemented, including giving ICANN a grade. "The second body that has oversight over this is the US government by the nature of the contract with us," he said. "Now, if you remove the US government what you have left is the IAB process. Is it visible? Is it transparent? Can anybody review it? The answers to these questions will determine if that's sufficient or if it needs to be enhanced."

Chehadé added that there is a similar oversight relationship with the Number Resource Organization (NRO), which represents the Regional Internet Registries (RIRs) that manage the IP addresses. He also added that instead of creating a formal board to oversee ICANN, which manages the domain names, he believed that there likely needed to be an additional audit capability to satisfy the NTIA requirements. The bottom line is that the NTIA has opened up the process for the Internet governance network itself to define the appropriate model for governing these shared Internet resources.

Expand the Role of the Internet Governance Forum

It is also important to understand that while many of the "big P" policy issues require legislative and educational activities, they will also require technical solutions, such as those that improve the privacy and security of Internet

users. In short, resolving many of these policy issues can only be done at the intersection of policy, technology and development. This means that the Internet governance network needs to bring together policymakers, civil society, Internet organizations and the private sector in order to address a number of policy-related issues.

To this end, there will likely be calls to expand the role of the IGF, primarily for the purpose of getting more government, private sector and developing country participation as well as to provide more specific leadership or guidance on Internet governance challenges. To cite one example, Vint Cerf and two colleagues from Google, Pat Ryan and Max Senges, have been circulating a paper in which they propose that the IGF become the major vehicle for resolving Internet policy-related issues.[52] While it's not clear what will happen in this area, it is likely that the IGF can play an important role in bringing all the critical parties together in a manner that facilitates complex global problem solving.

Nitin Desai, who developed the concept of Fuzzy Law and has been instrumental in the development of the IGF, said that the IGF "was an experiment. It was a multi-stakeholder forum within the UN....There were cultural adjustments that had to be made. Diplomats who were used to certain habits of debate often had to change when they interacted with the IG community. The Internet technical community found some of the ideological debates amusing...and the corporate sector was used to much more decisive functioning....One of the challenges was to get people to accept these cultural differences and adjustments. One of the successes of the IGF was that we did establish and create lines of communication between people who normally did not talk with one another. That was its success."[53]

Interestingly, while Desai sees the IGF's role expanding, he does not see the IGF becoming a decision-making body within the Internet governance network. He said, "I would expect IGF to move beyond being a deliberative forum to something that makes stronger recommendations to the different actors—the governments, the corporations, the Internet technical community and other stakeholders. What I would not wish to see is some attempt at trying to negotiate standards....The Internet already has a good system of building consensus and standards setting which needs to be preserved."

Stakeholders Shift by Issue

The multi-stakeholder model shifts on an issue-by-issue basis in the policy arena. This is an enormously important distinction. The stakeholder group typically remains relatively static, albeit quite broad, for technical and operational issues. For example, every one of the Internet organizations (the I* orgs.) engages with governments, civil society and/or individuals, as well as the private sector. While these engagements differ by organization or issue, in general most of the key stakeholders at any point in time are involved in the process, which has resulted in the enormous success of the Internet. One example of this success can be seen in the rapid growth in the population of users (although everyone would like it to be faster, the growth in number of

Internet users reflects the fastest growing communications medium ever). Growth has also come as platforms spread, easily encompassing voice, video and the rapid advent of mobile. The multi-stakeholder Internet governance ecosystem has grown and expanded in response to need and interest, itself becoming stronger even in the face of such rapid development.

The opposite is true in the "big P" policy arena. Each issue has many sets of stakeholders, often with diverse or competing values, political beliefs or social mores, and many of the policy issues confer economic advantage at both corporate and national levels. Furthermore, many of these issues can only be resolved with the participation of the web of legal jurisdictions at local, state, national, regional and international levels. Clearly, this necessitates open, accessible and easily adaptable processes. This is where multi-stakeholder, self-governing networks are playing a central role in transforming how we solve global policy problems.

Choice Should Remain the Defining Principle for Governing the Internet.

Choice and openness are highly contested principles, but they are essential to realizing the Internet's true potential. After all, one global, open Internet is a much more fertile domain for innovation and progress than one balkanized into regional subnets, where only some people have access to all of the world's online information. China, Russia and other authoritarian regimes don't support this vision because they must contend with the Internet's democratizing effects as increased scrutiny by citizens, both at home and abroad, undermines their ability to act in isolation and without criticism from the international community. On the other hand, such regimes have little choice but to count on information technology to drive economic growth in the 21st century. And, the rapid economic growth that many authoritarian countries desire is likely to trigger the very internal forces that will see authoritarian regimes crumble under the weight of their citizens' aspirations for a voice in their governance.

It's in the best interests of the international community to safeguard and promote the very qualities of openness and choice that have underpinned the Internet's remarkable growth to date. Indeed, it is worth emphasizing that the strength and competitive advantage of democratic states and free market economies lie in their rules-based, accountable and open systems, and in the values and standards that support them. As the Internet is woven into every fabric of life and the economy, it is essential that the principles that shape Internet governance mirror those of democratic states and not the opaque and capricious alternatives being actively pursued by authoritarian regimes. It is the very qualities of freedom, openness, integrity and collaboration that provide the essential raw materials for building a sustainable global economy in which everyone can participate.

Multi-Stakeholder Governance Model Will Become Mainstream

In Don Tapscott's and Anthony Williams' *Macrowikinomics*, they identified five principles for the age of networked intelligence: collaboration, openness,

sharing, integrity and interdependence. These principles sit at the core of the Internet's multi-stakeholder governance model, which might be characterized as management by collaboration and consensus. As we've pointed out in this report, this model of management is distinctly different from management by command and control, which sits at the heart of management theory for the industrial era.

As the Internet grows, its multi-stakeholder governance ecosystem will continue to serve as the seminal model for Internet governance, and it will likely spread worldwide as a new model of governance that will redefine how citizens (stakeholders) interact with their local and national governments, as well as how governments themselves might interact among themselves.

It should now be clear that this global ecosystem ("The Internet Governance Network") is strong enough and sufficiently well positioned to take the next steps and address some of the Internet's thornier policy issues. This ecosystem depends on the underlying principles and values that have supported the Internet's remarkable growth and stability. These are supported by the Internet organizations (not surprisingly), but also by many governments and policy makers, by many from civil society, and critically by the many in the private sector—the primary builders of the Internet. The ecosystem also builds on the Tunis Agenda for the Information Society as a very useful roadmap, and on the significant learnings from the many Internet governance forums. An important hallmark of this ecosystem has been its openness and its ability to adapt and this will remain a critical requirement as we all work to increase participation, particularly from developing countries, in order to maintain the open global Internet for the billions still to come online.

Endnotes

Quotations in This Paper: remarks in this paper were derived from a primary interview with the quoted person, unless otherwise identified by an endnote. The date of the interview is cited.

1 Don Tapscott and Lynn St. Amour, "The Remarkable Internet Governance Network—Part I, Understanding How a Global Ecosystem Can Govern. http://gsnetworks.org/research_posts/the-internet-governance-network-part1/

2 http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

3 It is not true, as widely reported, that it was designed to prevent an enemy from knocking out the US's military communications system in a nuclear strike. Paul Baran mentioned that reason in a paper on developing a network for secure voice communications, which was published by the Rand Corporation in 1964. The paper proposed using a new communications technique, called packet switching, to create a secure network that couldn't be eliminated in a single strike. Baran's work influenced the Internet's developers, and Baran later developed Internet-related products. The Internet, however, was developed for different reasons by another group of computer engineers.

4 Barry M. Leiner, Vinton G. Cerf, et al., "Brief History of the Internet," Internet Society, 1996.

5 Ibid.

6 Ibid.

7 http://tools.ietf.org/html/rfc675

8 http://en.wikipedia.org/wiki/ARPANET

9 Here is a list of these regional networks: BARRNet, the Bay Area Regional Research Network in Palo Alto, California; CERFNET, California Education and Research Federation Network in San Diego, California, serving California and Nevada; CICNet, the Committee on Institutional Cooperation Network via the Merit Network in Ann Arbor, Michigan and later as part of the T3 upgrade via Argonne National Laboratory outside of Chicago, serving the Big Ten Universities and the University of Chicago in Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin; Merit/MichNet in Ann Arbor, Michigan serving Michigan, formed in 1966, still in operation as of 2012; MIDnet in Lincoln, Nebraska serving Arkansas, Iowa, Kansas, Missouri, Nebraska, Oklahoma, and South Dakota; NEARNET, the New England Academic and Research Network in Cambridge, Massachusetts, added as part of the upgrade to T3, serving Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont, established in late 1988, operated by BBN under contract to MIT, BBN assumed responsibility for NEARNET on 1 July 1993. NorthWestNet in Seattle, Washington, serving Alaska, Idaho, Montana, North Dakota, Oregon, and Washington, founded in 1987;NYSERNet, New York State

Education and Research Network in Ithaca, New York; JVNCNet, the John von Neumann National Supercomputer Center Network in Princeton, New Jersey, serving Delaware and New Jersey; SESQUINET, the Sesquicentennial Network in Houston, Texas, founded during the 150th anniversary of the State of Texas; SURAnet, the Southeastern Universities Research Association network in College Park, Maryland and later as part of the T3 upgrade in Atlanta, Georgia serving Alabama, Florida, Georgia, Kentucky, Louisiana, Maryland, Mississippi, North Carolina, South Carolina, Tennessee, Virginia, and West Virginia, sold to BBN in 1994; and Westnet in Salt Lake City, Utah and Boulder, Colorado, serving Arizona, Colorado, New Mexico, Utah, and Wyoming.

10 http://en.wikipedia.org/wiki/World_Wide_web

11 http://en.wikipedia.org/wiki/Common_Gateway_Interface

12 http://en.wikipedia.org/wiki/National_Science_Foundation_Network

13 http://www.wired.com/business/2012/04/epicenter-isoc-famers-qa-cerf/2/

14 http://en.wikipedia.org/wiki/National_Science_Foundation_Network

15 http://en.wikipedia.org/wiki/Network_Solutions

16 http://www.internetworldstats.com/emarketing.htm

17 http://www.bitlaw.com/internet/domain.html

18 http://www.icann.org/en/help/dndr/udrp/policy

19 http://www.internetsociety.org/wsis

20 http://en.wikipedia.org/wiki/Working_Group_on_Internet_Governance

21 Ibid.

22 http://en.wikipedia.org/wiki/Suicide_of_Megan_Meier

23 http://en.wikipedia.org/wiki/Berne_Convention_for_the_Protection_of_Literary_and_Artistic_Works

24 Don Tapscott and Anthony Williams, *Wikinomics: How Mass Collaboration Changes Everything*, Penguin, London, 2006.

25 Don Tapscott and Anthony Williams, *Macrowikinomics: Rebooting Business and the World*, Penguin, London, 2010.

26 Spam is one of the few technical terms that isn't an acronym. It was named for the famous canned meat products from Hormel, although it was supposedly adopted from a Monty Python sketch. For more on spam's derivation, see https://en.wikipedia.org/wiki/spam_(Monty_Python).

27 http://www.itu.int/pub/S-CONF-WCIT-2012/en

28 http://www.fiercegovernmentit.com/story/wcit-12-revises-international-telecommunications-treaty-without-us-approval/2012-12-16

29 Ibid.

30 http://www.cnn.com/2013/07/17/world/asia/philippines-cybersex-

trafficking

31 http://en.wikipedia.org/wiki/Edward_Snowden

32 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

33 http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

34 http://en.wikipedia.org/wiki/Pogo_(comic_strip)

35 http://www.huffingtonpost.com/don-tapscott/living-out-loud-should-we_b_1532563.html

36 "A Vitual Counter-Revolution," *The Economist*, 10 September 2010. http://www.economist.com/node/16941635

37 https://opennet.net

38 Don Tapscott and Lynn St. Amour, ibid.

39 http://en.wikipedia.org/wiki/Net_neutrality

40 http://gigaom.com/2014/01/14/breaking-court-strikes-down-fccs-net-neutrality-rules/

41 Interview with Nitin Desai, January 3, 2014.

42 http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

43 Ibid.

44 http://netmundial.br

45 http://www.internetsociety.org/promoting-use-internet-exchange-points-guide-policy-management-and-technical-issues

46 http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

47 http://dailycaller.com/2014/03/15/ex-bush-admin-official-internet-giveaway-weakens-cybersecurity-opens-door-to-web-tax/#ixzz2w3BSVnp0

48 http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

49 https://www.internetsociety.org/sites/default/files/is-internetresources-201308-en.pdf

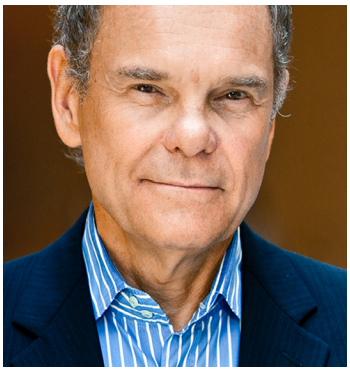
50 http://tools.ietf.org/html/draft-iab-iana-framework-01

51 http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

52 Vint Cerf, Pat Ryan and Max Senges, Internet Governance Is Our Shared Responsibility, which is in draft form at this writing and is scheduled for publication in I/S: A Journal of Law and Policy for the information Society.

53 Interview with Nitin Desai, January 3, 2014.

About the Authors



Don Tapscott is Executive Director of the *Global Solution Networks* program. As one of the world's leading authorities on innovation, media and the economic and social impact of technology, he advises business and government leaders around the world. He is CEO of the think tank *The Tapscott Group* and has authored or co-authored 14 widely read books. In 2013, the Thinkers50 organization named him the 4th most important living business thinker. He is Adjunct Professor of Management for the Rotman School of Management and the Inaugural Fellow of the Martin Prosperity Institute, both at the University of Toronto.

Lynn St. Amour is President and CEO of Internet Matters, an Internet consulting company. She served for 13 years as President and CEO of the Internet Society (ISOC), a global non-profit dedicated to the open development, evolution and use of the Internet. She joined ISOC in 1998 as Executive Director of its Europe, Middle East and Africa (EMEA) division, following senior positions in Europe and the US with AT&T and Digital Equipment Corp. She was appointed ISOC President and CEO in 2001.

Special thanks to principal researcher Steve Caswell. One of the early pioneers of the digital age, he was the founding editor of the *Electronic Mail and Message Systems* (EMMS) newsletter in 1977 and the author of the

seminal book *Email* in 1988. He also was a pioneer in ecommerce as one of the principal architects of the AutoSkill Parts Locating Network that has been used by auto dismantlers since the 1980s to buy and sell several billions of dollars of used auto parts. Today, he still follows the high tech industry very closely and teaches business and technology at Simi Valley High School in Simi Valley, CA.

About Global Solution Networks

Global Solution Networks is a landmark study of the potential of global web-based and mobile networks for cooperation, problem solving and governance. This research project is a deliverable of the GSN program, offered through the Martin Prosperity Institute at the Rotman School of Management, University of Toronto.

Program Management

Don Tapscott, Executive Director
Dr. Joan Bigham, Managing Director
Anthony Williams, Executive Editor

GSN Program Membership

Membership in Global Solution Networks offers unlimited access to gsnetworks.org program deliverables including project plans, research publications and multi-media presentations, all posted for member use, review and feedback. webinars on current research are held quarterly. Please visit our website at www.gsnetworks.org or contact info@gsnetworks.org for information on participation.

Ten Types of Global Solution Networks

MARTIN Prosperity Institute

Rotman School of Management UNIVERSITY OF TORONTO