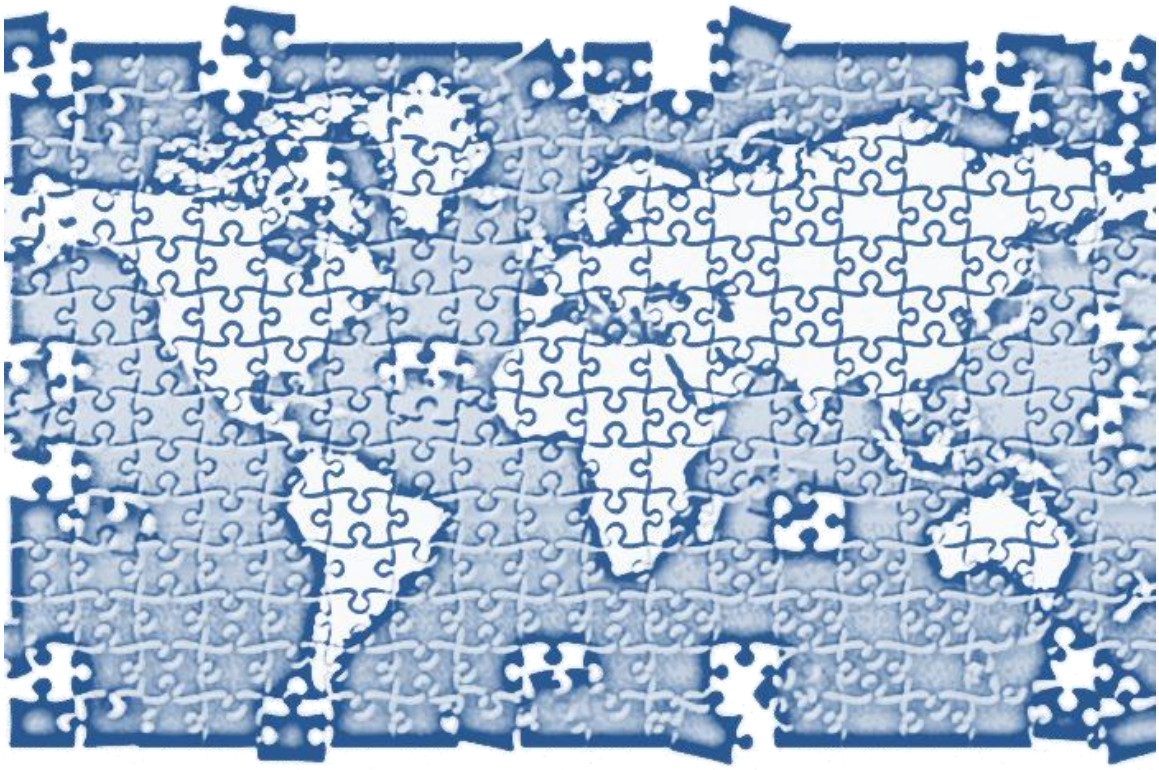


Internet Fragmentation

Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers

Jonah Force Hill
John F. Kennedy School of Government, Harvard University
Spring 2012

Acknowledgements

I'd like to thank Professor Joseph Nye for all his advice, support and feedback throughout the writing of this report; Scott Bradner for helping me work through all the technical and political issues at the IETF and other Internet governance forums; and the researchers at MIT's Computer Science and Artificial Intelligence Lab for their assistance with the IPv4/IPv6 and DNS issues.

This report would not have been possible without the generous support of the Minerva Initiative, which supports research conducted at the Massachusetts Institute of Technology and the Harvard Kennedy School through the Explorations in Cyber International Relations project.

[This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.]

HARVARD Kennedy School
BELFER CENTER
FOR SCIENCE AND INTERNATIONAL AFFAIRS
Information and Communications Technology and Public Policy

Table of Contents

Executive Summary

The Internet is at a crossroads. Today it is generally open, interoperable and unified. Tomorrow, however, we may see an entirely different Internet, one not characterized by openness and global reach, but by restrictions, blockages and cleavages. In order to help ensure that the Internet continues to serve as a source of global integration, democratization, and economic growth, American policymakers must be aware of the most significant technical, political and legal challenges to a unified Internet.

Drawing on a series of interviews with academics, government officials, and industry leaders, this report provides an account of the forces and actors that are threatening the global nature of the Net, and offers a brief sketch of the six distinct areas of greatest concern:

1. The Threat to the Domain Name System (DNS) – The DNS provides the translation service between a human-readable alphanumeric domain name, like WhiteHouse.gov, and its Internet Protocol (IP) address. In order for the DNS to function properly so that users can connect to a site they wish to view, Internet routers on the network must be configured to send and receive data from the canonical "root servers" coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN). There is concern that if countries decide to form national root servers apart from the ICANN-approved root, users of the Internet within those "seceding" countries could be effectively severed from the parts of the global Internet.

2. The Piecemeal Transition from IPv4 to IPv6 – IPv4, the predominant packetswitching protocol on the Internet today, uses a 32-bit address number, allowing for approximately 4.3 billion unique Internet addresses. This is an insufficient number of addresses given the past and anticipated future growth of the Internet. The successor to IPv4, IPv6 – which uses a 128 bit addressing system and thus has exponentially more address space - has not been rapidly adopted, even as free IPv4 addresses are becoming increasingly scarce. IPv4 and IPv6 are not immediately interoperable. If firms and countries fail to make the appropriate transition or to use effective translation tools, it is likely that applications will "break" and information will be lost across the IPv4/IPv6 divide.

3. Internet Censorship, Blocking and Filtering – In order to restrict access to, and to burden or prevent the publication of, certain types of information on the Internet, governments around the world are employing a variety of technical and legal tools to block websites and platforms and to remove online content. Through such tools as DNS filtering, IP blocking, distributed denial of service attacks (DDoS) and search result removals, governments are dramatically changing not only the way users connect to and participate in the wider global Internet, but how the Internet actually operates.

4. The Breakdown of Peering and Transit Agreements/Net Neutrality – Payments for data passed between large and small Internet Service Providers (ISPs)

is usually negotiated privately through bilateral interconnection agreements. Large ISPs generally pass data between one another without money changing hands. However, under the right set of circumstances, ISPs might discriminate against those services associated with the competition, thereby cutting service between users and certain sites affiliated with competing companies. Likewise, in opposition to the notion of "network neutrality," some ISPs may, believing that to do so would be in their business interests, choose to discriminate among the services they provide and to give priority to specific types of data. This too could have the effect of limiting the type of applications and services users could access based on the ISP to which they subscribe.

5. The Collapse of the Internet Standards Process – The organizations that design and promulgate the Internet's technical standards are coming under increased political pressure. Governments and firms assert that these organizations, which have been responsible for the Internet's core protocols and standards since the 1980s, are anarchic and discriminate against non-American technology firms. Regardless of the validity of these claims, there has been a concerted effort to take the standards-making power out of the hands of the established standards-making organizations, such as the Internet Engineering Task Force (IETF), and to give ultimate authority for standards to the United Nations and the International Telecommunications Union (ITU).

Advocates of a free and open Internet argue strenuously that a UN takeover of the standards process would be a disaster for the technical wellbeing of the Internet. But these advocates rarely discuss the implications of a continuation of the status quo. It may be that if the standards process continues without addressing its critics' concerns, we could see a country like China, or a coalition of countries, begin to mandate standards separate from the internationally accepted norm.

6. Local Privacy Regimes – In the effort to regulate online privacy and the way companies collect, store, and transfer citizens' personal information on the Web, governments around the globe are considering sweeping legislation. While increased legal protections for personal data may be a necessary part of the solution to the online privacy problem, there are mounting concerns that if many countries adopt their own unique privacy requirements, then every firm operating on the Internet could potentially be subjected to a multiplicity of inconsistent laws. If companies are unable to meet each country's differing requirements, either because those requirements are in conflict with one another or because of the added costs associated with meeting multiple disparate rules, then we could see firms pulling out of particular markets entirely.

The conclusions drawn from the analysis of these six case studies is, lamentably, not sanguine because there are now so many distinct forces and interests creating and multiplying the threats to a unified Internet. Policy makers who favor an interoperable system over more narrowly conceived governmental and corporate interests must begin now to address each of these problems, and to anticipate problems like these that may arise in the future, if irreparable balkanization is to be avoided.

Acronyms

APNIC	Asia Pacific Network Information Center
ASCII	American Standard Code for Information Interchange
ccTLD	Country Code Top Level Domain
CGN NAT	Carrier Grade Network Access Translation
CIDR	Classless Inter-Domain Routing
CIRP	Committee for Internet Related Policies
CNGI	China Next Generation Internet
CNIL	Commission Nationale de L'Informatique et des Libertes
DNS	Domain Name System
DS-Lite	Dual Stack Lite
FTC	Federal Trade Commission
FTP	File Transfer Protocol
gTLD	Generic Top Level Domain
HTTP	Hyper-Text Transmission Protocol
HTML	Hyper-Text Mark-up Language
IANA	Internet Assisigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IDNs	Internationalized Domain Names
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPv4	Internet Protocol Version Four
IPv6	Internet Protocol Version Six
ISOC	Internet Society

ISP	Internet Service Providers
ITRs	International Telecommunications Regulations
ITU	International Telecommunications Union
ITU-T	International Telecommunication Union Standardization Sector
IXP	Internet Exchange Point
LAN	Local Area Network
NAT	Network Access Translation
NRO	Number Resource Organization
ONI	OpenNet Initiative
RFC	Request for Comments
RIR	Regional Internet Registry
SIIT	Stateless IP/ICMP Translation
SIP	Session Initiation Protocol
TCP/IP	Transmission Control Protocol and the Internet Protocol
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
VPN	Virtual Private Networks
W3C	World Wide Web Consortium
WAPI	WLAN Authentication and Privacy Structure
WCIT-12	World Conference on Information Technology 2012

Introduction: A Fragmented Internet?

"It's really that the Web that is shattering into pieces here"
Author Josh Bernoff.[1]

"Sadly, it looks like the period in which the Internet functions seamlessly is over"
Internet Pioneer (now at Google) Vint Cerf.[2]

"We're facing a step-by-step balkanization of the global Internet"
Tim Wu, Professor of Law, Columbia University Law School. [3]

"Until now the Internet has been a nonhierarchical, seamless form of global communication. But all that is changing...it has become much like the rest of society—divided"
Journalist Rana Faroor.[4]

The Internet is at a crossroads. Today, it is generally open, interoperable and unified. Any Internet user can exchange email with more than two billion other global Internet users; entrepreneurs can launch services such as eBay and Amazon and quickly turn them into multibillion-dollar businesses; and people from all across the world can connect with others, share ideas, and improve democratic governance by means of social networking sites such as Facebook and Twitter.

Tomorrow, however, we may see an entirely different Internet, one not characterized by openness or interoperability. With more than two billion users currently connected, the Internet has grown by nearly five hundred percent in the past decade.[5] The locus of the Internet, so long dominated by Americans and the English-speaking world, is now shifting

[1] Bernoff, John. "Prepare for the age of the splinternet."
http://marketplace.publicradio.org/display/web/2010/01/27/pm-splinternet-q/
[2] Werbach, Kevin. (2008). "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart," 42. UC Davis L. Rev. 343, 402-05 (347)
[3] David, Bob. Rise of Nationalism Frays Global Ties, Trade, Environment Face New Threats; Balkanized Internet. The Wall Street Journal. http://online.wsj.com/article/SB120934738145948747.html
[4] Foroohar, Rana, "The Internet Splits Up," The Daily Beast (May, 2006)
http://www.thedailybeast.com/newsweek/2006/05/14/the-internet-splits-up.html
[5] Internet World Statistics, "The Internet Big Picture: World Internet Users and Population Stats."
http://www.internetworldstats.com/stats.htm

eastwards towards Asia, as Chinese Internet users now outnumber Americans and English is no longer the Internet's majority language.[6] Increases in computer network power, the spread of broadband connectivity, cloud computing, and the Internet of Things (IOT)[7] are all transforming the way Internet users connect to the network.

As a result of these and other fundamental changes to the Internet ecosystem, politics and economics are increasingly impinging on the Internet's interoperability and global nature. Over the past decade, an increasing number of journalists and academics have noted - often in alarmist terms - the ways in which national government polices, commercial interests, and other dynamic changes in the Internet are pulling the global network apart into various distinct, idiosyncratic "internets," threatening the innovation, economic prosperity, and global communication the Internet has provided over the past two decades.

Yet despite the proliferation of articles and commentaries on this "balkanization"[8] of the global Internet, there has been little consensus about which parts of the Internet are fragmenting, what changes in the Internet are causing the fragmentation to occur, and to what degree these processes should be a concern. This paper will seek to provide policymakers with an account of the most profound challenges to a unified Internet today, as well as some of the areas of potential future concern, including the threats to Domain Name System, the risks associated with the IPv4 to IPv6 transition, government-mandated Internet content filtering and blocking, risks associated with differentiated pricing schemes, local privacy regimes and potential legal challenges, and the interoperability problems that might arise from a breakdown the Internet standards process.

A NON-FRAGMENTED INTERNET?

In order to make sense of the forces that are dividing the global Internet today - and might further divide it in the future - it is first necessary to try to characterize what a "non-fragmented" Internet might look like. This initial step in the analysis is itself a challenging task because the Internet is an astoundingly complicated lattice of interconnected systems. It is often portrayed as a seamlessly integrated network, but this is in many ways a simplification of a much more nuanced reality. Like the railroad system and the electric power grid, the Internet is not a single system, but rather a number of separate networks; in the case of the Internet, the system consists of a collection of independent computer networks that coordinate and share information through common computing languages called protocols, forming what appears to be a seamless whole.

Not all networks are connected to the Internet in the same way; connectivity often depends upon network capacity and the network operator's preferences. It is not unusual, for instance, for organizations such as banks or power-stations to deploy their own internal

[6] Rose, Richard. (2011) "The Internet Goes EFL (English as a Foreign Language). Brookings Institution: Issues in Technology Innovation, Number 5.
http://www.brookings.edu/~/media/Files/rc/papers/2011/01_efl_rose/01_efl_rose.pdf

[7] ITU (2005) ITU Internet Reports 2005: The Internet of Things. Geneva: International Telecommunications Union. http://www.itu.int/publ/S-POL-IR.IT-2005/e

[8] For the purposes of this paper, I will use terms like "balkanization," "fragmenting," "splintering," "separating," etc. interchangeably.

computer networks using the Internet's core protocols (the Transmission Control Protocol and the Internet Protocol (TCP/IP)) and over the Internet's underlying physical infrastructure, while still restricting certain types of access from the outside, and from the inside of the network out. Things like Firewalls and Virtual Private Networks (VPNs) installed within and around networks can restrict or block certain types of information from getting in or out. Such access restrictions are normal and entirely appropriate given the security and privacy needs of certain types of organizations. Yet they also serve to illustrate the range of networks connected to the Internet and the problems associated with thinking of fragmentation of the Internet as a deviation from a seamless original.

Adding to the complexity, the Internet supports a diversity of applications and uses. Unlike the telephone network, which was designed exclusively for voice transmission, the Internet was not intended for any particular application. Instead, it was designed to be a general-purpose infrastructure over which any variety of computer applications could run, and for which no permission was required to join. This generality has allowed for the distributed creation of new applications and uses that the original Internet engineers could never have imagined. As a result, the Internet might be best understood as a multilayered mesh of the networks, hardware, software, applications, storage systems, fiber cables, radio frequencies, transmissions, switches, screens, businesses and people, rather than a unified homogenous network.

All this diversity of access and purpose makes the Internet hard to grasp and Internet fragmentation difficult to define precisely. Hence, there has been little consensus among those observers who point to the growing fragmentation of the Internet about what is actually breaking. The Internet is not - and has never truly been - an entirely seamless system without boundaries or limits,[9] or a single-purpose communication tool, so to say that is becoming less or more fragmented is immediately problematic. If we were interested in defining fragmentation of the telephone network, for instance, we would simply want to know the degree to which individuals could call one another. But with a utility such as the Internet, with no single intended use and differing levels of connectivity depending on the preferences of the network operators, it is hard to define unity versus fragmentation with any kind of specificity.

A SPECTRUM OF INTERNET FRAGMENTATION

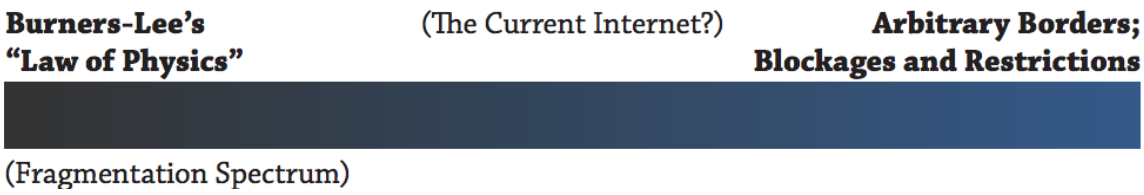
Accordingly, to take up the challenge of understanding the problem of Internet fragmentation, it is essential to develop a methodology to help us analyze the degree to which the Internet is either unified or fragmented, which parts of the Internet are fragmenting, and which actors and processes are actually causing the fragmentation to occur.

Looking first at the question of defining the degree to which the Internet is or is not fragmented, MIT Professor Tim Burners-Lee, in a lecture entitled "The End of the World Wide Web,"[10] provides a useful analogy that can help shape the discussion. He argues that the "laws" of the Internet should function like the laws of physics, i.e. the laws that exist in

[9] Except perhaps in its earliest days before commercialization. Scott Bradner, Interview, February 19, 2012
[10] Zittrain, Jonathan. Interview, November 1, 2011

one part of the Internet should apply everywhere on the Internet. Again, the Internet is not a single purpose infrastructure. But as Burner-Lee argues, an application should function at one point in the network as it does at any other; a website should look the same to a person in China as it does to a person in Chile. In other words, the experience of every Internet user should be the same regardless of geographic location, computer type, or any other distinguishing characteristic of the user.

Clearly, this "laws of physics" state does not currently exist in today's Internet and will likely never exist in the future given the technical and legal idiosyncrasies of communications systems and nation-states. However, Professor Burners-Lee's analogy nevertheless provides a useful standard against which we can develop a theory of Internet fragmentation. Placing the Internet on a spectrum, Burners-Lee's "laws of physics" standard sits at one end. On the other end we have an entirely fragmented Internet, with "arbitrary and consistent borders," blockages, and restrictions.[11] A fragmented Internet, then, is an Internet in which the experience of one Internet user is radically different from another's. It may be difficult to place the current Internet at any specific location on the spectrum, but having a linear model to work with provides us with a means to orient ourselves, and to gauge the direction – to the right (fragmented) or left (unfragmented) of what I'll call the "Fragmentation Spectrum" - in which a particular intervention or change in the ecosystem might push the Internet.



A LAYERED APPROACH TO LOCATING FRAGMENTATION

Once having visualized the Fragmentation Spectrum, our next analytical task, defining which parts of the Internet are moving us to the right of the Fragmentation Spectrum, requires that we develop a system to classify different parts of the Internet. Luckily, we have an existing model (or perhaps it is more precise to say "set of models") to which we can turn. Computer scientists tend to break down the Internet into a series of discrete analytical categories using a common method of classifying systems called "layering." In these models, different parts of the Internet are grouped together into different sub-categories, or layers. There are a number of different Internet layering systems and scholars may choose to use different systems depending on the type of analysis being done or according to personal preference. For this paper, I will make use of MIT's David Clark's simple four-layer approach, one of the more widely used models, but by no means the prevailing one.[12]

[11] Zittrain, Ibid.

[12] For instance, Harvard Law School Professor Yochai Benkler uses a three-layer model in his "Wealth of Networks: How Social Production Transforms Markets and Freedom," Yale University Press (2000) and University of Pennsylvania Law Professor Kevin Werbach opts for a four-layer model in "A Layered Model for Internet Policy," Journal on Telecommunications and High Tech Law, Vol. 1, No 37, 2002. The Open

The four-layer model, like the other layering models, is generally represented as a vertical stack. At the bottom of the stack lies the "physical layer," which includes all the Ethernet wires, fiberoptic cables, DSL lines, and other hardware through which the electronic data "packets" travel. Immediately above the physical layer is the "logical layer," which encompasses the core Internet Protocols (TCP/IP), the Internet services, such as the Domain Name System (DNS), and all the applications such as the World Wide Web and email. Next, situated on top of the logical layer, is the "information layer," which is comprised of all of the online content, including blogs, news, video and music that is communicated between and among users. And at the very top of the stack is the "people layer," the individuals, companies, and governments that actually participate in the Internet's growth and use. Often this "people layer" is left out of the layered model, but for our purposes its inclusion is essential to permit us to categorize the laws, human institutions, and decisions that ultimately are causing much of the Internet's fragmentation to occur.

Layer	Description
People	Individuals, Businesses, Gov't, Law
Information	Blogs, Wikipedia, Youtube
Logical	
Application	Web, Email
Services	Domain Name Service
Internet	TCP/IP
Physical	Ethernet, DSL, Fiber Optic

(Layered Model)

A CLASSIFICATION OF ACTORS AND FORCES

It is also useful to classify what actors and what processes are affecting the changes that are causing the Internet to fragment. Here, again borrowing from existing models and the tools of analysis used in political science, we can further refine our the examination of fragmentation by subdividing the actors and processes into different categories. Broadly, the actors affecting changes in the Internet fall into regulatory actors, such as the national governments that promulgate and enforce laws, the international organizations that adopt and enforce international agreements and develop norms, and the individuals who inform the decisions of their respective governments; business actors, such as the Internet Service Providers (ISPs) that connect customers to the Internet and technology companies that design new products and services for the Internet; and the end-users, the individuals, businesses, and other purchasers and users of Internet products and services. The processes shaping the future of the Internet may be usefully categorized as technological changes, like the creation of a revolutionary new Internet protocol or the exhaustion of Internet Protocol Version 4 (IPv4) address spaces (to be discussed below); and social and market changes,

Systems Interconnection (OSI) seven layer model, developed by the International Organization for Standardization (ISO), is also frequently used in Internet discussions.

such as a change in consumer preference from one application or platform to another or demographic changes among Internet users.

Regulatory Actors	National Governments, International Organizations (UN, ICANN), Individuals, Standards Organizations
Business Actors	ISPs, Technology Providers, Industry Associations
End-Users	Individuals, Businesses
Technological Changes	New Applications, IPv4 to IPv6, Internet of Things, Cloud Computing
Social and Market Changes	Changes in Preference, Demographic Changes

(Actors and Forces)

With these three matrixes to guide the analysis - the Fragmentation Spectrum, the Internet Layers Model, and the Classification of Actors and Forces – we now have the analytical tools to permit an analysis of trends that may lead increasingly to the balkanization of the Internet.

II. Fragmentation at the Logical Layer: The Domain Name System

> "The principal example of Internet...balkanization [is] the fragmentation of the address space."
>
> Keven Werbach, Professor of Law, University of Pennsylvania Law School[13]

A TACIT AGREEMENT

The Internet famously has no central government.[14] The early Internet engineers incorporated into the Internet's architecture their belief that connecting people together and enabling them openly to share ideas was an objective that should be encouraged; consistent with that objective, the early designers insisted that governments should have a very limited role in regulating the Internet. Accordingly, they designed protocols and routing systems so that they could function with little centralized operation or control. However, there were and still are a few key Internet services that depend on centralized oversight and management; one the most important of which is the Domain Name System (DNS), and it is here that many observers fear the Internet could fragment.

Virtually every Internet-connected device is assigned a 32 bit numerical label called an Internet Protocol address (IP address), much like a phone number or a home address. Websites and users generally prefer not to identify themselves by these 32 bit series of zeros and ones that constitute the IP address, however, and instead choose to be identified by more user-friendly and memorable alphanumeric domain names like Amazon.com or Ebay.com. The DNS, which functions much like the "white pages" of the Internet, provides the translation service between these human-readable alphanumeric domain name and the 32 bit IP addresses.[15]

The DNS also – to use another imperfect but useful analogy – works like the Internet's automated telephone operator. Every time an Internet user's web browser requests information from a webpage, or an email is sent over the network, a user's Internet Service Provider (ISP) queries a nearby Internet router (located at various physical points around the Internet) for information about a given domain name. The router then translates the domain name into an IP address by retrieving IP address mapping information from one of many

[13] Werbach, Kevin. (2008). "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart," 42. UC David L. Rev. 343, 402-05 (355)

[14] See Goldsmith, Jack and Wu, Tim. (2006) "Who Controls the Internet? Illusions of a Borderless World." Oxford University Press

[15] For an overview of the DNS System, see Karrenberg, Daniel (2004) "The Internet Domain Name System Explained for Non-Experts," ISOC Member Briefing #16, The Internet Society

global "root servers," the canonical IP address directories which categorize and organize the "generic top-level domains" (gTLD) such as .gov and .com, and the "country code domains" (ccTLD), such as .br for Brazil and .fr for France. If the router is able to locate the requested IP address from the DNS root registries, it will make the translation, identify the next step on the way to the IP address of interest, and return that information to the user so the link between the user and the site can be made.

The root zone servers and the root zone files are coordinated under the umbrella of the Internet Corporation for Assigned Names and Numbers (ICANN), pursuant to a contract with the U.S. Department of Commerce. As long as all ISPs and Internet routers connect properly to the ICANN-approved root servers, every active domain name will accurately represent a unique point on the Internet. However, an ISP or a routing system could be configured to point to a root directory that is not endorsed by ICANN.[16] If an ISP did so, its users might be sent to an entirely different website than the one they thought they were requesting, or might receive no information back at all. Users would have no way of knowing that they had been sent to the wrong site because the redirection would appear seamless.

This redirection tends not to happen because governments, ISPs, and other network operators have abided by a tacit voluntary agreement to participate in the global Internet system and to direct traffic to ICANN-operated root servers. This agreement, however, is not legally binding; the current DNS system does not preclude alternative registries from forming.[17] In fact, there are today a number of these alternative DNS root servers, often known by the shorthand "alt roots,"[18] which serve Internet traffic to alternative gTLDs. There are a number of reasons why these alt roots exist: sometimes they are operated for idealistic or ideological reasons; sometimes they are designed to create the type of secure and separated networks that were mentioned above. Some of these alt roots are approved by ICANN and are assigned IP addresses and correctly direct traffic; some of them are designed specifically as a protest to ICANN's monopoly on the DNS.[19]

For the purposes of understanding Internet fragmentation, these existing alt roots currently do not seem to present a substantial risk to the interoperability of the Internet, or move the Internet to the right of the Fragmentation Spectrum, since they are used by very few users

[16] There are currently eleven ICANN-approved "root zone operators" which manage the root servers: VerSign, Information Sciences Institute, Cogent Communications, the University of Maryland, NASA, Internet Systems Consortium, Inc, U.S. Department of Defense, U.S. Army Research Lab, Autonomica/NORDUnet, RIPE NCC, WIDE Project, and ICANN itself. As of 2007, there were actual servers located at more than 130 locations within 53 countries worldwide. ISOC, "DNS Root Name Servers Explained." http://www.isoc.org/briefings/019/ (September, 2007)

[17] Although the Internet Architecture Board warns strongly against this in RFC 2826 "IAB Technical Comment on the Unique DNS Root" (2000): "Put simply, deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers. This does not preclude private networks from operating their own private name spaces, but if they wish to make use of names uniquely defined for the global Internet, they have to fetch that information from the global DNS naming hierarchy, and in particular from the coordinated root servers of the global DNS naming hierarchy." http://tools.ietf.org/html/rfc2826

[18] See "Public-Root," operated by the Internet Names Authorization and Information Center, http://public-root.com/ and "Unified root" http://www.unifiedroot.com/ for examples.

[19] "IAB Technical Comment on the Unique DNS Root," http://tools.ietf.org/html/rfc2826

around the world and direct a trivial fraction of Internet traffic.[20] The more serious concern is that at some point in the future a national government or alliance of governments could break off from the ICANN-approved root servers and form their own national or regional roots that were not connected to the rest of the DNS. This has yet to happen in any meaningful way, but there has been one prominent example of the potential for governmental withdrawal from the ICANN root, the DNS internationalization debate of the 2000s.

DNS INTERNATIONALIZATION AND THE THREAT OF UNILATERAL ROOT SERVERS

The American engineers who first designed the DNS built the English language directly into the routing protocols. Generic top-level domain names, for example, are abbreviated versions of English words, for example ".com" is short for commercial and .org for organization. More significantly, the character set used for Internet addresses was exclusively ASCII, a character standard designed for English and other languages based on the Roman alphabet. In order properly to connect to the DNS, websites in languages with non-Roman-based scripts had to transliterate their domain names into Roman characters. Thus, for Internet users around the world to access the wider global Internet they had to have some familiarity with a foreign script, which is no trivial matter for residents of countries, like Thailand and China, with radically different writing systems.

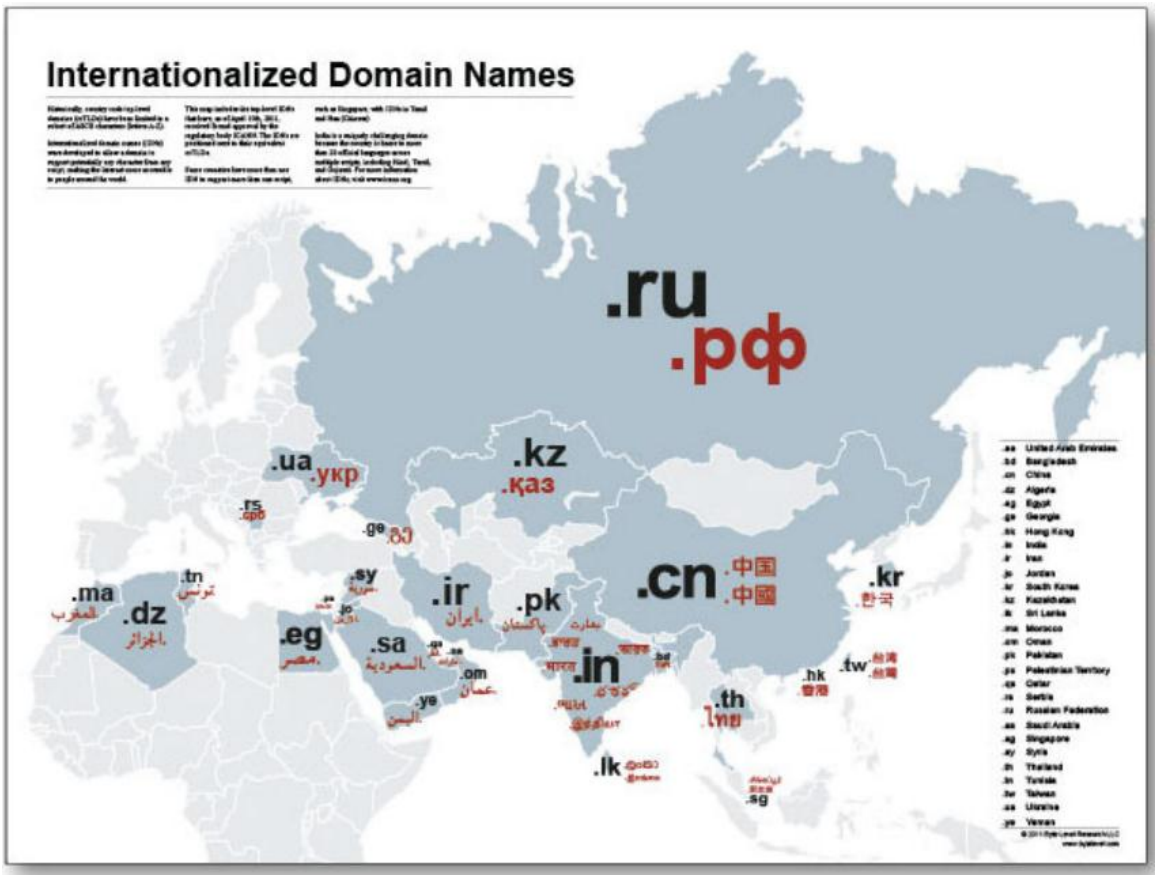
These countries pushed for years for the development of ccTLDs and gTLDs in their own native scripts. Yet even though the Internet Engineering Task Force (IETF) had developed the technology necessary for non-Roman scripts as early as 1996,[21] ICANN was remarkably slow to move forward.[22] With pressure mounting, and with ICANN dragging its feet, China took unilateral action in 2005-2006 and began to experiment with a parallel root designed for Chinese character gTLD names. In addition to the .CN domain assigned by ICANN, China began to experiment with Chinese character gTLDs .中国 (.china), .公司 (.company) and .网络 (.network).[23] There were also reports that Iran, Saudi Arabia and Egypt were considering taking similar steps if ICANN did not push ahead in responding to the concerns of their Internet-connected populations.[24]

This unilateral move by China presented a serious challenge to the authority of ICANN, and in turn to the entire global Internet system as it is known today. In order for users to access

[20] Berger, Arthur, Interview at Massachusetts Institute of Technology, November 1, 2011
[21] Dürst, Martin J. (December 10, 1996). "Internet Draft: Internationalization of Domain Names". The Internet Engineering Task Force (IETF), Internet Society (ISOC). http://tools.ietf.org/html/draft-duerst-dns-i18n-00
[22] Levine, John. (2007) "Splitting the Root: Its Too Late"
http://www.circleid.com/posts/splitting_root_too_late/; and Bradner, 2011
[23] MacKinnon, Rebecca. (2006) China's New Domain Names: Lost in Translation.
http://www.circleid.com/posts/chinas_new_domain_names_lost_in_translation/
Bradner, Scott. Interview, October 14, 2011
http://english.people.com.cn/200602/28/eng20060228_246712.html
[24] Marsan, Carolyn Duffy. 2006. "Native Language Domains Threaten Net, Networked World,"
http://www.networkworld.com/news/2006/032706-icann-internationalized-domain-names.html?page=1

the new Chinese gTLDs, routers would need to have been reconfigured to connect to these new Chinese root servers. This would have meant that Chinese computers and routers would have been configured to Chinese root servers while the rest of the world would have been configured to the ICANN root. If the Chinese Internet authorities in charge of this new root and its routing tables were unable or unwilling to coordinate with ICANN, or visa versa, it very well might have been impossible for Chinese users to access the outside Internet or for users outside of China to reach Chinese sites. In effect, the new root would have created separate, un-interoperable Internets, divided at the logical level.

In response to China's experimental alternative root work, as well as to continuing pressure from other countries demanding the implementation of Internationalized Domain Names (IDNs), the ICANN Board, meeting in South Korea in October 2009, approved the "IDN ccTLD Fast Track Process" to allow countries and territories to submit requests to ICANN for ccTLDs in scripts other than those with ASCII characters, including Chinese, Arabic and Cyrillic. Subsequently, at a Singapore conference in 2011, ICANN further approved a gTLD Program to allow for the addition of IDN gTLDs into the root zone.[25]



The decision to move ahead with IDNs was an immensely important – and politically and technically challenging - step towards maintaining interoperability and a unified Internet. It stopped for now the Chinese and others from moving ahead with their own unique, disconnected root servers. But the threat of a parallel root in the future should not be

[25] ICANN, IDNs: Internationalized Domain Names, http://www.icann.org/en/topics/idn/

dismissed. A number of countries continue to resent the perceived American domination of ICANN, IANA and the DNS system in general. As an example of this continuing tension over the authority of these American-based institutions, the Indian government at the 2011 General Assembly of the UN in New York formally called for the creation of an entirely new body, the Committee for Internet Related Policies (CIRP) to take control of the DNS (in addition to other Internet governance powers) out of the hands of ICANN and IANA. The CIRP would exist under the United Nations, be run by staff from the UN's Conference on Trade and Development arm, and would report directly to the UN General Assembly.[26] The Chinese government, too, has tried to galvanize support to transfer authority to the International Telecommunications Union (ITU), an existing U.N. information and communications body.[27]

Many observers of the Internet have also noted that the new IDN system, as it is being implemented by ICANN, is fraught with other IDN-related problems that could spiral out of control if not properly addressed.[28] There are intellectual property issues: several languages contain strings of characters that have equivalent or near equivalent meanings, which might confuse users trying to reach certain websites. For instance, some Chinese characters have two representations – a traditional Chinese character and a simplified character. Simplified characters are rarely used in Taiwan or Hong Kong and thus could lead to divisions within the Chinese-language diaspora. There are also security concerns: because certain letters in one script look identical to letters in another script, there are concerns that criminals will try to "spoof "[29] websites and steal users' sensitive information.[30] For instance, a Greek letter "a," which looks indistinguishable from a Roman script "a," could be inserted into a link for a fake version of genuine domain name, such as paypal.com. A user would have no idea that he had just clicked on a link to a fake site, since the paypal.com domain name on the browser would look identical.[31]

The future of the DNS is uncertain. Many academics and policy makers believe China was not entirely serious about creating a separate root but was instead raising the threat to pressure ICANN to take more immediate action.[32] Most also agree that the creation of a separate root system in the future is an unlikely outcome, at least in the near and medium

[26] McCarthy, Kieren. (2011) "India formally proposes government takeover of the Internet" http://news.dot-nxt.com/2011/10/27/indiaproposes-government-control-internet; for the actual text of the proposal, see: http://igfwatch.org/discussion-board/indias-proposal-fora-un-committee-for-internet-related-policies-cirp

[27] Bradner, Scott. Interview, Ibid

[28] International Chamber of Commerce (2003), "Issue Paper on Internationalized Domain Names," Department of Policy and Business Practice, Commission on IT and Telecoms, Task Force on the Internet and IT Services. There are also concerns about the number of TLDs that are now permitted by ICANN. Companies are being forced to purchase a huge number of domain names to protect their copyrighted names.

[29] A tactic by which a criminal provides a user with a link to what looks like familiar website but is in fact fraudulent to steal information.

[30] International Chamber of Commerce (2003), Ibid.

[31] It should be fairly easy to protect against this specific type of fraud since browsers should be able to restrict mixed-character domain names from being opened. But criminals will likely get creative in their spoofing efforts in ways not yet anticipated. David Clark, Interview November 22, 2011

[32] Palfrey, John. Interview. Scott Bradner Interview. Jonathan ZIttrain Interview

terms since the incentives to do so are too few and the potential damages would be too great to justify it.[33]

But the Internationalization episode did demonstrate the fragility of the DNS system. If issues like the security or perceived fairness of the DNS system are not properly addressed in the future, countries may feel that it is in their best interest to withdraw, form their own secure root, and go it alone. Such a move could be potentially disastrous for the Internet's interoperability, and cause a significant shift of the Internet towards the right of the Fragmentation Spectrum, balkanizing the Internet at the logical, service level.

[33] Ambassador David Gross, Interview on October 6, 2011. Ambassador Gross did suggest that the DNS is not a sustainable system in the long-term.

III: Fragmentation at the Logical Layer (Application and Internet): The Transition from IPv4 to Ipv6

"In the process of IPv4 space exhaustion, a partial transition to IPv6 could lead to Internet balkanization."
Arthur Berger, MIT Computer Science and Artificial Intelligence Laboratory[34]

THE EXHAUSTION OF INTERNET PROTOCOL VERSION 4 (IPV4)

The standard Internet Protocol adopted by the Internet research scientists in the late 1970s was called Internet Protocol Version 4 (IPv4).[35] As noted above, the IPv4 standard made use of an IP addressing system with a 32-bit address space, allowing for around 4.3 billion (2^32) unique addresses. At the time, the Internet was still a noncommercial network used by only a small number of scientists on a few American university and research computers,[36] so the 4.3 billion addresses seemed nearly inexhaustible, even profligate. Laura DeNardis, in her book chronicling the history and politics of the Internet Protocol, Protocol Politics, argues that "in retrospect, [the choice to include so many addresses] showed tremendous foresight and optimism about the Internet's future."[37] But, as Internet use expanded exponentially and the network no longer connected only to personal computers but also began to incorporate mobile phones, Voice over Internet Protocol (VoIP), and other devices such as printers, the seemingly inexhaustible address space turned out to be imminently exhaustible.

The Internet standards community identified this potential depletion of the IPv4 addresses as a critical concern in the early 1990s, even though at that time fewer than 15 million individuals used the Internet.[38] The IETF, which defines many of the key Internet protocols, including the Internet Protocols, responded to the impending address shortage by developing a next generation Internet Protocol - Internet Protocol Version 6 (IPv6) - which was formally adopted in the mid-1990s as the official replacement to IPv4.[39] IPv6 "solves" the address space problem by providing a 128-bit number address space, or 340 undecillion (2^128) unique addresses.

---

[34] Berger, Arthur. Interview at Massachusetts Institute of Technology, November 1, 2011
[35] RFC 791 DARPA Internet Program Protocol Specifications (1981) "Internet Protocol." http://www.ietf.org/rfc/rfc791.txt
[36] RFC 760 DARPA DOD Standard "Internet Protocol" http://tools.ietf.org/html/rfc760
[37] DeNardis, Laura. (2009) "Protocol Politics: The Globalization of Internet Governance." MIT Press
[38] Ibid
[39] IP version 5 was deployed in some US military systems, but never made serious commercial inroads. For all the RFCs for IPv6 see the IETF working group page at: http://datatracker.ietf.org/wg/ipv6/

STAVING OFF THE INEVITABLE

Obtaining IPv4 addresses is growing increasingly difficult.[40] On February 3, 2011, the Number Resource Organization (NRO), the official representative of the five Regional Internet Registries (RIRs) that are responsible for distributing IP addresses to countries in specific international geographic regions, announced that the free pool of IPv4 spaces had been "fully depleted," after IANA had allocated its last IPv4 spaces to the Asia Pacific Network Information Center (APNIC), the RIR is responsible for assigning IP addresses in Asia.[41] This does not mean that all the IPv4 address spaces have been handed out, since the five RIRs still have yet to themselves hand out the IPv4 spaces they had been allocated by IANA.[42] But APNIC is now rejecting some applications for new IPv4 spaces, and for those applications that are granted, will allocate only 1024 address blocks, clearly not enough space to meet the needs of Asia's growing Internet user community.[43]

Yet even in the face of the dire NRO announcement, IPv6 implementation is still only in its infancy. As of October 2011, only about 3% of domain names and 12% of the networks on the Internet can support IPv6,[44] and less than one twentieth of one percent of Internet traffic is running "native" IPv6, or entirely on IPv6 addresses.[45] Given all the warnings about the impending depletion of IPv4 space since 1990, one would have thought that ISPs and others would have acted with more urgency to make the transition and begin adding IPv6 addresses to their networks.

There are a number of reasons why ISPs have been so slow to respond. First, there is no central body in the U.S. or internationally to enforce IPv6 adoption. Most countries have left the transition up to the free market and the discretion of the network providers. The Internet Society (ISOC), in anticipation of the second World IPv6 Day, tentatively scheduled for June 2012, has been encouraging ISPs to transition at least 1% of their addresses to IPv6, but even that small a fraction has been an enormous challenge.[46]

Second and more importantly, there are strong economic incentives for ISPs to avoid making the transition. IPv4 and IPv6 cannot directly interoperate; a server running on an IPv4 address space cannot immediately share information with a computer using an IPv6 address, unless the former is configured for IPv6 functionality. Since there are so few IPv6

---

[40] It is difficult to know when exactly the day will come when the available space will dry up, since IP address assignment is a intermittent process. For years experts have tried to calculate a depletion-date, only to find their predicted date come and go. Cisco released a report in 2005 suggesting that IPv4 spaces would run out as early as 2009. Hain, Tony. (2005) "A Pragmatic Report on IPv4 Address Space Consumption" The Internet Protocol Journal, Volume 8, Number 3
http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html

[41] Free Pool of IPv4 Address Depleted, Number Resource Organization (February 3, 2011)
http://www.nro.net/news/ipv4-free-pool-depleted

[42] Arthur Berger notes that "ARIN will allocate to an organization only enough addresses to accommodate three months of growth; APNIC is now rejecting some applications, and for those applications that are granted, will allocate only 1,000 addresses." Interview, 2011

[43] Arthur Berger notes that there is now a growing market for IPv4 addresses, even though they had been free previously.

[44] Leber, Mike (2011) "Global IPv6 Deployment Progress Report." Hurricane Electronic Internet Services (Backbone Provider) http://bgp.he.net/ipv6-progress-report.cgi

[45] Labovitz, Craig (2010) "IPv6 Momentum?" http://www.circleid.com/posts/ipv6_momentum/

[46] See "World IPv6 Day" http://www.worldipv6day.org/

addresses now deployed around the Internet, there is a collective action problem among ISPs. All ISPs would all be better off if they all made the transition and could easily communicate with one another, but with IPv6 providing few added benefits to the user, no single ISP has a market incentive to act first and make the costly, yet necessary transition.

With so few IPv6 addresses now on the network, ISPs must use translation services to bridge the two standards. Translation tools such as Network Access Translation (NAT) devices like NAT64,[47] Stateless IP/ICMP Translation (SIIT) services, and Dual Stack Lite (DS-Lite) configurations[48] are some of the most popular, but these services are expensive and the cost is almost always borne by the service providers.[49] Additionally, all of the backend software used for network administration and operation assumes IP address spaces with 32 bits. Updating this software is again expensive and without immediate (or even potentially long-term) benefits.[50] In short, ISPs, applications providers, and website owners need to make the transition but have seen no immediate incentive to incur the expense as of yet.

As a result, ISPs and others have gone to great lengths to avoid switching over and have taken a variety of stopgap measures to postpone the transition. Among other measures, ISPs have been using Classless Inter-Domain Routing (CIDR) systems to extend the life of the pool of IPv4 addresses.[51] More often, they have deployed Carrier Grade Network Access Translation (CGN NATs) boxes along their networks, in a process often dubbed "IP-masquerading," to expand the number of users who can log on to a single public IPv4 address. CGN NAT boxes turn private IPv4 local area network (LAN) addresses, or IPv6 addresses used within a given ISP, into public IPv4 addresses, thereby permitting the sharing of small pools of unique public addresses among many users, in effect expanding the number of users who can make use of a particular IPv4 address space.

These steps, while delaying the inevitable move to IPv6, are only drawing more use out of already existing IPv4 addresses through a reshuffling of resources; they do not deal with the underlying challenge of IPv4 space exhaustion.[52] Moreover, these stopgap measures may also create performance problems. NATs in particular are problematic since they add yet

---

[47] RFC 6146 "Statefull NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers." http://tools.ietf.org/html/rfc6146

[48] RFC 6333 "Dual-Stack Lite Broadband Deployment Following IPv4 Exhaustion" http://tools.ietf.org/html/rfc6333

[49] ISPs and other groups have also a vested interest in maintaining IPv4 if they have an excess number of IPv4 address spaces, thinking that in the future they may be able to sell them in a future IPv4 market.

[50] RTI International estimates (back of the envelope) that the transition for US government networks to IPv6 could alone cost upwards of $25 billion dollars. http://www.networkworld.com/newsletters/isp/2006/0320isp1.html; http://www.rti.org/pubs/IPv6_cost-benefit.pdf

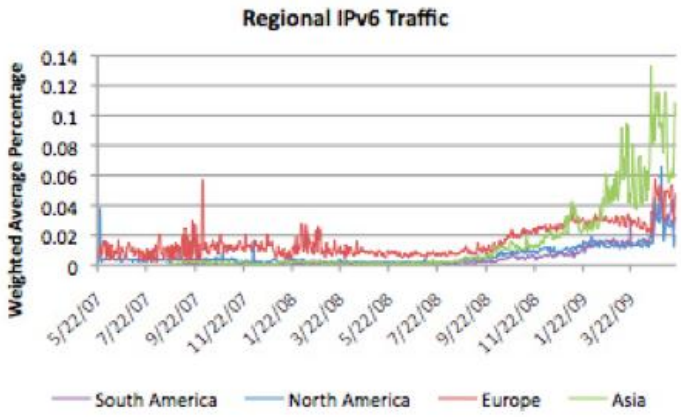
[51] CIDR is a fairly complex system that restructures the IPv4 routing tables and the way IPv4 addresses are distributed. The system allows for more precise allocation of IPv4 space so that organizations are given excess IP numbers.

[52] The creation of markets to buy and sell extra, unused IPv4 spaces has been proposed many times as a temporary solution to the exhaustion problem, but has been met with much skepticism for the following reasons: the concept of legal ownership of IP addresses is poorly defined in international law and it remains unclear who would arbitrate disputes, since IP addresses need to be allocated in blocks, there would be severe operational problems in the routing tables if smaller groupings were sold, the cost of changing from one set of IP addresses to another is quite high.

another layer of address translation to the network[53]and thus have the potential to "break some applications."[54] For example, a number of application layer protocols - such as the File Transfer Protocol (FTP) and the Session Initiation Protocol (SIP) used for video streaming, VoIP, and other file transfer services - depend on a constant connection with a specific IP address; the shifting and "masquerading" of IP addresses through CGN NATs can lead to a break in the connection.[55] These disruptions may not bring about a balkanization in the Internet as obvious and as damaging as those that might be brought about through a split DNS root zone, for instance, but they certainly act to push the Internet farther towards the fragmented right-end of the Fragmentation Spectrum. And as the depletion of IPv4 reaches a critical point, we may see more and more of these types of application breaks and degraded service.

INTERNET BALKANIZATION FROM IPV6

The real threat to the Internet's unity and interoperability relating to the IPv4/IPv6 transition comes not from these application breaks but from the dramatically different IPv6 adoption rates among different regions and countries.[56] In the figure to the right (provided by NRO) we can see that Asia has jumped far ahead of Europe and North America in percentage of IPv6 traffic. This difference is primarily the result of a relative scarcity of IPv4 spaces in Asia, since the continent was allocated a disproportionately small number of IPv4 addresses compared with its population and Internet growth rates.[57] The Asian Regional Internet Registry (APNIC), the RIR responsible for Asia, has now entered a stage called "hyper-austerity," in which there are only a few free IPv4 spaces left.[58]



Anticipating this impending crisis beginning in 2000, the governments of China, Japan, Korea, and India[59] all established national strategies to upgrade to IPv6.[60] Beyond addressing

[53] Wilson, Carol (2011) "The Ugly Side of IPv6: Carrier Grade NATs." http://www.lightreading.com/document.asp?doc_id=208857
[54] Berger, ibid.
[55] In June 2010, CableLabs, Time Warner Cable Roger's Communications found that video streaming, VoIP (Skype), video gaming and peerto-peer file sharing were all aversely impacted by NATs. For a technical explaination see RFC http://tools.ietf.org/html/draft-donley-nat444-impacts-03
[56] Berger, Ibid.
[57] Berger, Ibid.
[58] APNIC's IPv4 Pool Usage (2011) http://www.apnic.net/community/ipv4-exhaustion/graphical-information

the IPv4 exhaustion problem, these countries' governments also saw an economic opportunity in IPv6: by taking the lead in this new arena, they could become the new global leaders of IPv6 products and expertise in what is otherwise an American dominated Internet industry.

China in particular has made IPv6 implementation and the development IPv6 technology a cornerstone of its forward looking Internet strategy, since it more than any other country is short on IPv4 spaces. China has only approximately 100 million IPv4 spaces for a country of more than 1.3 billion people and over 400 million Internet users.[61] The Chinese government has sought to expand IPv6 to six nationwide backbone networks – connecting at two Internet exchange points (IXPs) in Beijing and Shanghai - to provide IPv6 to over 20 major metropolitan areas and 300 academic, industrial and government research centers around China, as part of their China Next Generation Internet (CNGI) initiative.[62] China has reportedly invested $200 million into the program.[63]

This decision by Asian countries to move ahead with IPv6, given their shortage of IPv4 space relative to the number of users and the desire to take the lead in a budding technology industry looks to have been a sound decision. Yet it is also presents a serious threat to American commercial competitiveness in the next generation of Internet technologies. Equally important, at least for the purpose of maintaining a unified and interoperable Internet, the decision presents serious potential impediments to the free flow of information. If the United States and other countries with a greater surplus of IPv4 spaces do not make the transition at the same rate as Asia, or fail to make the technical adjustments necessary for translation, there may be serious interoperability problems within the crucial East/West Internet relationship.

[59] PC World Magazine, India. (2010) "India Gears for IPv4 to IPv6 Switch." http://www.pcworld.in/news/india-gears-ipv4-ipv6-switch-30412010

[60] DeNardis, Laura. (2009), Ibid; Shinde, Jayesh "India Gears for IPv4 to IPv6 Switch" http://www.pcworld.in/news/india-gears-ipv4-ipv6-switch-30412010

[61] In 2004 China had 6 (/8) blocks of IPv4 spaces allocated to it by IANA, approximately 94 million spaces. APNIC (2004). "IP Addressing in China," first appearing in Issue #12 of APSTER, APNICS quarterly newsletter. http://www.apnic.net/community/about/internet-governance/articles/ip-addressing-in-china-2004#ipv4-left

[62] Worthen, Ben (2006) "Internet Strategy: China's Next Generation Internet" CIO Chief Information Officer Magazine. http://www.cio.com/article/22985/Internet_Strategy_China_s_Next_Generation_Internet_

[63] Berger. Ibid.

IV: Fragmentation at the Information Layer: Internet Censorship and Website Blocking and Filtering

"What we once called a global Internet is becoming, for many practical purposes, a collection of nation-state networks, still linked by the Internet protocol, but for many purposes, separate."
Larry Lessig, Professor of Law, Harvard Law School[64]

"If every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning."
Vint Cerf, early Internet pioneer (now at Google)[65]

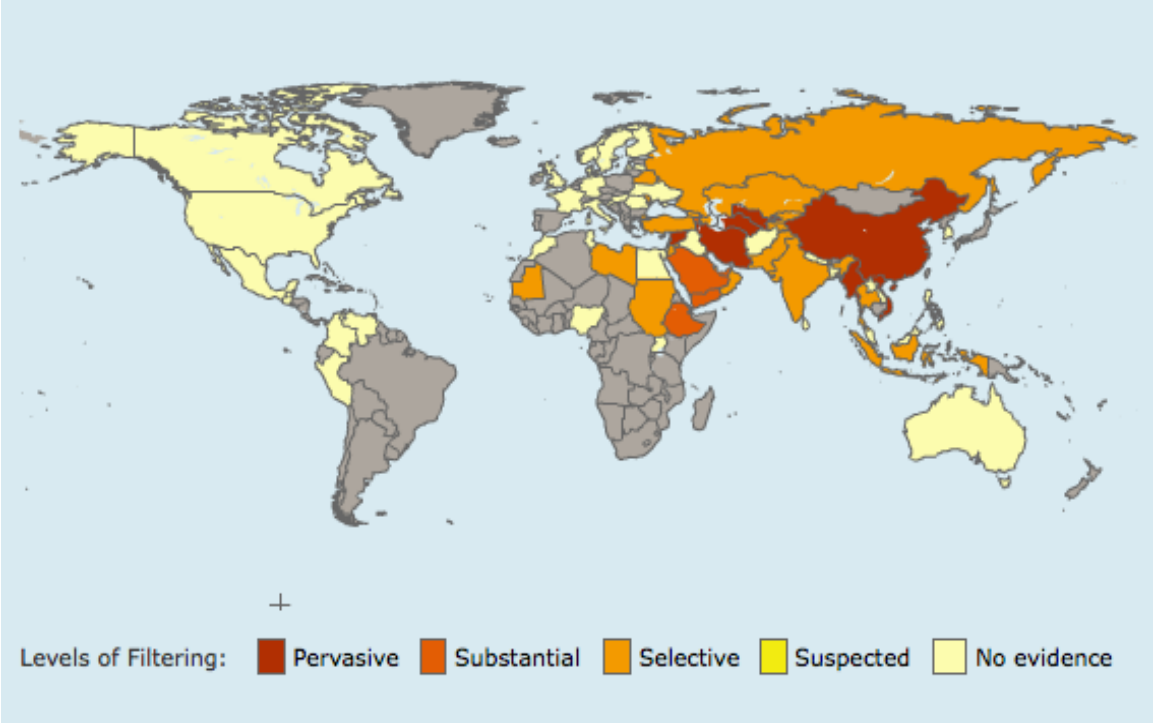
CONTROLLING THE BORDERLESS

When the Internet first became commercially available in the 1990s, governments had very little role in regulating its structure or the content of the information it delivered to its users. Yet as it grew as an engine of global economic growth, and as the threats to that growth from hacking into institutional computer networks, spam, phishing scams, and other forms of cybercrime became more prevalent, governments began to look for ways to control cyberspace. And, of course, criminality was not the only, or even the primary, concern of governments: state security, and the position of states' ruling elites, were and are seen to be jeopardized by the nearly limitless social and political mobilizing features of the Internet.

Efforts by governments to control the uses and users of the Internet have taken on many forms. The International community accepts a variety of controls as legitimate: for example, few would oppose increased protection for children from predators online[66] or anti-botnet programs.[67] Other efforts at control however, particularly those aimed at restricting political discourse and suppressing the expression of ideas—restrictions that are nothing less than governmental censorship—are more controversial. Not surprisingly, governments engaged in restricting the expression of and access to political ideas justify their

[64] Lessig, Lawrence (2004) "The Balkanization of the Internet" http://www.lessig.org/blog/2004/08/the_balkanization_of_the_inter.html
[65] Quoted in Zittrain, Jonathan (2005) "The Balkanization of the Broadband Internet." The Broadband Explosion: Leading Thinkers On The Promise Of A Truly Interactive World, Harvard Business Press
[66] Although it should be noted that child pornography is often used an excuse for increased government control of the Internet, even in the United States. See the Center for Democracy and Technology (CDT) report on the Pennsylvania blocking case https://www.cdt.org/pr_statement/cdt-challenges-pennsylvanias-net-blocking-law
[67] See Japan's Cyber Clean Center, https://www.ccc.go.jp/en_ccc/

policies—while responding to their critics, principally in the West—by echoing arguments raised against criticism of more traditional censorship. Censoring governments such as China insist that civil liberties notions (a principal, if not the exclusive basis for the argument in favor of an open and unrestricted Internet) are a Western construct that cannot claim universal moral applicability; moreover, state sovereignty permits, even compels, those governments to restrict expression of ideas if they deem it to be in their national interest to do so.



Yet censorship on the Internet is not the same as censorship of other media forms, and is not susceptible to the same sovereignty arguments that apply to restrictions on what can be written in newspapers and said on television. Sovereignty is essentially a matter of exclusive power exercised within borders, while the Internet is quintessentially a borderless system.[68] The Internet was designed so that any user could exchange information with any other user regardless of physical location. Accordingly, it not only challenges traditional ideas of state sovereignty, it presents profound problems to governments wishing to control that exchange of information. Content that is illegal in Country A may be still available to Country A's Internet users from sites hosted overseas, where the content is legal and where Country A may have little influence. To restrict its citizens' access to the offending content, Country A's censors must not only employ "extensions of pre-existing media or telecommunications

[68] For more see: Kobrin, Stephen J. (2001) "Territoriality and the Governance of Cyberspace," Journal of International Business Studies, Vol. 32 No. 4 687 – 704; and, Goldsmith, Jack and Wu, Tim, "Who Countrols the Internet? Illusions of a Borderless World." Oxford University Press, 2006

regulatory regimes"[69] to control locally generated content, but must also use increasingly sophisticated blocking and filtering tools to restrict information coming from outside.

The debates about the appropriate role for governments in cyberspace bring up complex legal questions of jurisdiction and national sovereignty, questions that will continue to cause tension in international forums and confound legal experts for years.[70] But since the borderless nature of the Internet is causing some governments to put up walls to restrict access to content not only within but outside their geographic borders, and since virtually every government with a stake in the Internet is now engaged in some kind of censorship online,[71] it is important to note how these efforts at censorship are balkanizing the Internet at both the information and logical layers, and pushing the Internet, with certain authoritarian countries like China, Iran and Saudi Arabia in the lead, forcefully towards the right of Fragmentation Spectrum. As Ronald Deibert notes, "the Internet a user connects to and experiences in Canada is now far different than the Internet a user experiences in Iran, China, or Belarus."[72] This is perhaps the very definition of a fragmented net.

THE MANY METHODS OF GOVERNMENTAL INTERNET CENSORSHIP

Much has been written on the topic of Internet censorship, most importantly as a result of the research efforts of Reporters Without Borders,[73] Freedom House,[74] the U.S. Department of State's NetFreedom Task Force, and the OpenNet Initiative (ONI) (a collaboration of the Citizen Lab at the University of Toronto, the Berkman Center for Internet and Society at Harvard, and the SecDev group at Cambridge University).[75] The research conducted by these organizations has shown the wide variety of tactics governments have employed to prevent, take down, and block what they find to be objectionable material on the Internet.

---

[69] Zittrain and Palfrey, "Internet Filtering: The Politics and Mechanisms of Control" in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., "Access Denied: The Practice and Policy of Global Internet Filtering," (Cambridge: MIT Press) 2008

[70] See Zittrain, Jonathan (2003) Be Careful What You Ask For, in Who Rules the Net? Internet Governance and Jurisdiction. (Adam Thierer et al. eds., 2003)

[71] For instance, of the 37 countries examined in the most recent Freedom House Internet Freedom study, fifteen were found to engage in "substantial blocking of politically relevant content," such as "independent and opposition news outlets, international and local human rights groups, and individual blogs, online videos, or social networking groups." And "even in more democratic countries—such as Brazil, India, Indonesia, South Korea, Turkey, and the United Kingdom—internet freedom has been increasingly undermined" by "legal harassment, opaque censorship procedures, and expanding surveillance." Freedom House's "Freedom on the Net, 2011: A Global Assessment of Internet and Digital Media Freedom" Report at http://www.freedomhouse.org/template.cfm?page=664

[72] Deibert, Ronald J. (2008) "The geopolitics of Internet Control: Censorship, Sovereignty and Cyberspace." In the Chadwick, Andrew and Howard, Philip N. editors, "Routledge Handbook of Internet Politics." Routledge Publishers (p. 1)

[73] For Reporters Without Borders Internet page see: http://en.rsf.org/internet.html

[74] Freedom House (2011)

[75] See Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, (Cambridge: MIT Press) 2008 and, Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Controlled: The Shaping of Power, Rights and Rules in Cyberspace. (Cambridge: MIT Press) 2010

The Open Net Initiative lists four broad strategies governments are using in their efforts to prevent their local populations from viewing suspect content:

1) Technical Blocking	The use of technical tools to prevent access to specific online content or applications
2) Search Result Removals	The omission of websites from search results of major search engines.
3) Take-Downs	Government regulators force website hosts to remove materials from the web, by either legal means or by the threat of violence
4) Induced Self-Censorship	Intimidation (threats of take downs, civil and criminal penalties) leads to self censorship

(Strategies of Censorship)

Of the four strategies employed by governments, only the first two – Technical Blocking and Search Result Removal - constitute forms of Internet fragmentation as we have defined it above. Certainly all four strategies can be remarkably effective in preventing access to information. Nevertheless, Take-Downs and Induced Self Censorship do not fundamentally change the way information is transmitted or received on the Internet, but rather only affect what information is available. Thus these methods do not fundamentally create "arbitrary" or "consistent" borders on the network. This is a subtle distinction but an important one, if we are concerned about the forces actually altering the structure of the Internet and moving it towards the right-hand side of the Fragmentation Spectrum. Therefore, it is the first two that we will now consider.

TECHNICAL FILTERING, BLOCKING AND SEARCH RESULT REMOVALS

A state wishing to block its citizens' access to certain parts of the Internet has several technical options at its disposal: filtering and misdirection of the DNS, blocking of IP addresses, or blocking at the Uniform Resource Locator (URL). Each of these techniques has its own strengths and weaknesses.[76] The choice of technique depends upon the capability of the government that requests the filtering—the reach of its authority and influence, the laws in place and degree to which the government can alter or circumvent those laws, the people against whom the can enforce its wishes, and how much it is willing to spend to accomplish its filtering. "Other considerations include the number of acceptable errors, whether the filtering [is meant to] be overt or covert, and how reliable it is (both against ordinary users and those who wish to bypass it)."[77]

Most states with advanced filtering regimes make use of all four of the methods. IP address blocking is perhaps the simplest tool, however. IP packet filtering takes two forms, TCP/IP "header" filtering and TCP/IP "content" filtering. An IP packet consists of a header and the data the packet carries (known as the payload), much like an address on an envelope and the contents of the envelope. Internet routers must inspect the packet header to determine

[76] Steven Murdoch and Ross Anderson provide a useful comparison of the most common types of filtering in "Tools and Technology of Internet Filtering" in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, (Cambridge: MIT Press) 2008

[77] Murdoch and Anderson, 2008. Ibid. (p. 58-59)

where to send the packet. To prevent targeted websites from being accessed, however, routers can be configured to drop packets destined for IP addresses on a government blacklist. There are problems with this type of filtering, however, since blocking based solely on IP addresses - which may provide other services like email - will make all services on each blacklisted host inaccessible. Additionally, header filtering only looks at the header and not what is actually contained in the payload. This can be a problem if governments do not have a full list of banned IP addresses. In response, governments are using increasingly sophisticated versions of deep packet inspection (DPI) techniques to drop packets based on the type of materials contained in the payload.

Many governments prefer to use URL filtering,[78] when possible, to help avoid the over-filtering or under-filtering problems seen in IP or DNS filtering tools.[79] URL filtering targets the code associated with the series of dashes and hyphens that make up the Uniform Resource Locator and the Hyper-Text Transmission Protocol (HTTP). A government looking to block access to certain types of content will provide ISPs with a list of specific key words, such as "Tiananmen" or "Dalai Lama." If those key words or some permutation of them are found within the request of a user in her URL, the ISP will configure the network to drop the request. In the event of a drop, all that the user will see is an error message saying that the website could not be found. To illustrate, the ONI observed in its recent study that the United Arab Emirates and Syria blocked every site found within the Israeli ccTLD space, such that no pages from any domain ending in ".il" were accessible there. Conversely, the URL block also had perhaps the unintended consequence of blocking traffic "in both directions: someone from a ".il" address may have a hard time accessing content in the UAE as a result of the filtering there."[80]

DNS filtering, likewise, blocks users' access to certain sites, but here the blockage is carried out not through the URL, but through a disruption of the Domain Name to IP address translation and query process. As described above, the DNS translates and locates IP addresses so that packets can be exchanged. If a government wishes to block certain sites, it can simply provide a list of prohibited domain names to the ISPs, and instruct them to tamper with the DNS routers on their network, redirecting the routing to the wrong location. A user attempting to access one of those prohibited domains will be unable to access the site because the DNS routing tables will be corrupted and the packets will be sent to the wrong address, or dropped altogether. Without IP address translation, again the requesting computer's browser will display an error message.

As a final method of filtering, governments may also instruct major Internet portals, such as search engines, to exclude prohibited websites from their web-searches. Since search engines are the primary means by which users look up information on the web, omitting

---

[78] Pakistan has recently published a public tender for the "development, deployment and operation of a national-level URL filtering and blocking system" that "should be able to handle a block list of up to 50 million URL's" "Pakistan Builds Web Wall Out in the Open" http://www.nytimes.com/2012/03/03/technology/pakistan-builds-web-wall-out-in-the-open.html?ref=technology

[79] Palfrey, John. "Local Nets on a Global Network: Filtering and the Internet Governance Problem," in Jack Balkin et al. "The Global Flow of Information" NYU Press (p. 6)
Also note that The Protect Intellectual Property Act (PIPA) and the Stop Online Piracy Act (SOPA) could have allowed the U.S. government to mandate D.N.S. blocking—the technique that Iran had used—to prevent Americans from seeing unauthorized postings of copyrighted material on social-media or search-engine sites.

[80] Murdoch and Anderson, (2008), Ibid. (p. 38)

certain sites or pages with banned keywords serves to render sites and information inaccessible to the average user. In 2009, for instance, a secret memo circulated around the censorship department of the Chinese company Baidu (China's most important search engine) provided specific lists of topics and words that would be censored and blocked, and guidelines for how to mask the censorship so that it would be less obvious.[81]

BALKANIZATION OF CONTENT

Scholars and observers of the Internet often point out that "as a practical matter, it is easy for a state to carry out technical Internet filtering at a simple level, but very tricky – if not plain impossible – for a state to accomplish in a thorough manner."[82] They observe that no matter how sophisticated government censorship regime may be, individual users will always be able to outsmart the censor and access the materials they want to view. But as MIT's Ethan Zuckerman,[83] Rebecca McKinnon and others have pointed out, circumvention, especially as it is usually accomplished, is an ineffective way to promote Internet openness and counter balkanization. Average users do not have the technical skills - out of Chinas 500,000,000 users fewer than 1% use these tools to get around censorship[84] - or the wherewithal to use the most popular circumvention tools. Even if they did, to accomplish that end they would need more bandwidth than is currently available. Remember that twelve of the twenty most popular sites globally are entirely blocked in China;[85] in order to provide proxy services to all of China's users would be operationally impossible.

Internet censorship presents perhaps the most striking example of Internet balkanization because it is the only example of premeditated balkanization. As the recent statements by Iran's Head of Economic Affairs, Ali Aghamohammadi, about the Iranian government's plan to create a separate, "genuinely halal network" indicate,[86] some governments are actively trying to sever themselves off from the rest of the Net. In their efforts to deny their citizens access to information and applications through filtering and blocking, governments have in effect balkanized the net at all the layers of the Internet stack: people, information, logical and even physical (governments will often set up their physical Internet infrastructure to enhance the ability to censor information).[87] Not surprisingly, in a conflict between the benefits of Internet interoperability and concerns of state security, the Internet is the inevitable loser.

---

[81] "Baidu's Internal Monitoring and Censorship Document Leaked" http://chinadigitaltimes.net/2009/04/baidus-internal-monitoring-and-censorship-document-leaked/

[82] Zittrain, Jonathan and Palfrey, John in: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, (Cambridge: MIT Press) 2008 (p. 30)

[83] Zuckerman, Ethan. (2010). "Internet Freedom Beyond Circumvention." http://www.ethanzuckerman.com/blog/2010/02/22/internet-freedom-beyond-circumvention/

[84] McKinnon, Rebecca (2012). "Consent of the Networked: The Worldwide Struggle for Internet Freedom." Basic Books (Advanced Copy)

[85] Dong, Donnie (2010). "Google's Angry, Sacrifice and the Accelerated Splitting Internet." (Referenced by Ethan Zuckerman) http://english. blawgdog.com/2010/01/googles-angry-sacrifice-and-accelerated.html

[86] Rhodes, Christopher and Fassihi, Farnaz "iran Vows to Uplug Internet" Wall Street Journal, http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html#ixzz1YJmxxqiG

[87] In China, for example, global Internet connects to the Chinese Internet through only eight gateways which are easily filtered. McKinnon 2012, Ibid.

V. Fragmentation at the People and Physical Layers: the Breakdown of Peering and Transit Agreements and Net Neutrality

"The need to mitigate congestion, rationalize Internet access pricing and streamline may result in "balkanization" of the Internet, i.e., the isaggregation of a "network of networks" into an amalgam of networks, with varying degrees of accessibility to other networks."
Robert Frieden, Professor of Communications, Pennsylvania State University[88]

THE PROBLEM WITH PEERING

As described above, the Internet emerged in a minimally regulated environment. Regulation was also nominal in the business relationships that formed between and among the different network providers. This was especially true for the business relations in the United States between those ISPs that maintain the Internet "backbones," the principal data pathways and core routers on the Internet. Internet backbones are like the Internet's core arteries; most Internet traffic will at some point travel on one, if not multiple, backbones on its journey across the Internet. Very little traffic can travel across the Internet on a single backbone without having to hop on to another backbone at some point along the way. ISPs must accordingly collaborate and share their resources to ensure that all data is sent and received properly.

This collaboration is usually done through private bilateral interconnection agreements. These agreements general fall into two broad categories: peering agreements and transit agreements. In a peering agreement, the two networks exchange traffic without any money switching hands between the two ISPs. The assumption is that the two networks gain roughly equal benefits from the relationship and that metering and billing for traffic passing in each direction only adds unneeded complexity and transaction costs to an already complicated technical arrangement. In a transit relationship, alternatively, one network, generally the smaller of the two, pays the larger network for the service of delivering packets across its backbone. These arrangements may be messy and problematic at times, but they have worked astoundingly well up to this point.

However, as University of Pennsylvania Law School Professor Kevin Werbach argues, "the incentives to preserve peering, and the broader linkage it promotes across the physical layer, are diminishing," and "changes in the backbone market…could break down the traditional

88 Frieden, Robert (1998). "Without Public Peer: The Potential Regulatory and Universal Service Consequences of Internet Balkanization," Virginia Journal of Law and Technology, 3 VA J.L. & Tech 8 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=102927

peering equilibrium."[89] If, for instance, as Werbach observes, Verizon and AT&T, two of the largest ISPs and the only large backbones to last mile connectivity,[90] were to decide to peer only with one another and refuse to peer with anyone else, say, because of concern among established telephone network providers over the threat of VoIP services, other major backbone providers would likely follow suit and form their own exclusive peering relationships. If this were to happen, "the new backbone ecosystem would be dominated by, in all likelihood, two to three independent archipelagos, involving a combination of backbone, last-mile, and content/information service assets."[91]

If these different backbone providers had strong business ties with large websites, such as Facebook, or applications, such as Skype, they might give preferential treatment to those companies. It is unlikely that this new monopolistic arrangement would cause traffic to be dropped entirely, since the market forces against that would be too high, but "the quality of access, and the menu of offerings available to customers, would vary depending on their choice of access provider."[92]

Regulators would certainly have cause to step in and intervene in a case such as this,[93] but if they were unable to do so (perhaps as a result of a political environment hostile to enforcement of the anti-trust laws), a situation could emerge in which backbone conglomerates would provide connectivity to established applications and services like email, but discriminate against those services associated with the competition.

THE NETWORK NEUTRALITY DEBATE

In addition to the problem of restrictive peering arrangements, there are other potential business changes that could fragment the Internet, specifically through differentiated pricing for different types of data. The Internet's protocols and routing mechanisms were designed to be indifferent to the type of data being sent over the network.[94] This was an intentional design priority of the early Internet engineers, helping to ensure that the routers that transmitted the data could focus on delivering the packets successfully. When the Internet was commercialized, this indifference to the data captured within a packet translated into a system in which ISPs charged the same rate for all Internet traffic regardless of what was inside the packet. Today, for the most part, this uniform pricing structure has continued.

But there have been calls for some time to alter this system. In the growing debate over 'network neutrality," a number of ISPs have argued that the system is outdated and they

[89] Werbach, Kevin. (2008). "The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing it Apart," 42. UC Davis L. Rev. 343, 402-05 (p. 370)
[90] The network wiring or wireless signal that actual connects to an individual user's house or businesses.
[91] Werbach (2008) Ibid. (p. 371); whether such combinations would survive anti-trust scrutiny is of course problematic
[92] Ibid (p. 372)
[93] In the late 1990s, for instance, "Sprint and WorldCom abandoned their proposed merger largely because the Department of Justice announced its intention to block the combination for promoting excessive consolidation of the Internet backbone." Werbach, 273 See Complaints at 9-11, United States v. WorldCom, No. 00-CV-1526 (D.D.C. June 26, 2000)
[94] Clark, David D. and Marjory S. Blumenthal, "The end-to-end argument and application design: the role of trust," Internal Draft MIT CSAIL

should be able essentially to discriminate among the services they provide, and to give priority to specific types of data. AT&T and Verizon and some cable companies would like to substitute net neutrality with "a pricing schedule where, besides the basic service for transmission of bits, there will be additional charges by the Internet operator for services applied to the originating party (such as Google, Yahoo or MSN)."[95] The ISPs argue that since certain applications such as online video require enormous bandwidth, hosts ought to be charged more for the increased data flow.

Proponents of network neutrality argue, to the contrary, that data-type indifference is a fundamental design principle of the Internet, a principle that has allowed for competition and all the positive externalities associated with it. As Tim Burners-Lee writes, "it is the cleanness of that design, and the strict independence of the layers, which allowed the Internet to grow and be useful. It allowed the hardware and transmission technology supporting the Internet to evolve through a thousand-fold increase in speed, yet still run the same applications. It allowed new Internet applications to be introduced and to evolve independently."[96]

Scholars, including prominently Phil Wieser, Tim Wu, Chris Yoo, and Barbara van Schewick, have done extensive work analyzing the pros and cons of net neutrality, and have attempted to propose solutions that would suit both its supporters and opponents.[97] However, it remains to be seen what ISPs and regulators will ultimately decide. Either way, this debate, while raging in other countries as well, is a domestic business and legal matter, and as such does not present as fundamental a threat to the Internet's unity as do the previously discussed threats. However, if companies with monopolistic ambitions are allowed to discriminate to such a degree that users are unable to access content because of the cost or the unwillingness of ISPs to connect to the competition, we could see the Internet shifting towards the right of the Fragmentation Spectrum.

[95] Economides, Nicholas and Tag, Joacim. (2011) "Network Neutrality on the Internet: A Two Sided Market Analysis." NET Institute Working Paper 07-45, NYU Law and Economics Research Paper 07-40
[96] Burners-Lee, Tim. "Neutrality on the Net." http://dig.csail.mit.edu/breadcrumbs/node/132
[97] See Weiser, Phil. (2003) "A Third Way on Network Neutrality." Harvard Journal of Law and Technology, Vol. 17, No. 1, Fall; Yoo, Chris. (2004) "Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate." Journal of Telecommunications and High Technology Law, Vol. 3; van Schewick, Barbara. (2007) Toward an Economic Framework for Network Neutrality, Journal on Telecommunications and High Technology Law, Vol. 5

VI: Fragmentation at the Logical Layer: Internet Technical Standards

"The Internet we know today could not have come about without open, interoperable, global standards. After we have worked so long and so hard together to ensure that...products from all vendors around the world would be compatible with each other, I am surprised and disappointed by the action taken by the ITU-T, which takes us off the path of global interoperability."

Russ Housley, Chair of the Internet Engineering Task Force (IETF), in reference to the split MPLS standard.[98]

STANDARDIZED CONFUSION

The Internet is held together as a globally interoperable platform through its common set of technical protocols, message formats and computer languages, also known as Internet standards. Internet standards - such as IPv4 and IPv6, Hyper-Text Mark-up Language (HTML), Hyper-Text Transfer Protocol (HTTP), and Border Gateway Protocol (BGP) - set the normative technical specifications for communication on the Net. By ensuring the Internet's reliability, and by providing a predictable marketplace for goods and services, a common set of global Internet standards has allowed the Internet to rapidly expand around the world.

Yet the organizations and processes that decide which protocols and languages will be accepted as the international standards are not without their critics. A growing chorus of national governments has argued that the organizations and processes that lead to standardization are both outmoded and inequitable. They argue that the current process unfairly favors American firms, that it produces standards with insufficient built-in security, and that it produces standards that allow for a degree of freedom fundamentally at odds with the social norms of some nonwestern nations.[99] Today as a result of these concerns, the technical design decisions that were historically the sole province of engineers and academics have increasingly come under the political pressures of governments seeking to influence and reform them.

---

[98] Internet Society Statement, February 21, 2011. "IETF and Internet Society Statement relating to today's ITU-T SG15 decision that will lead to non-interoperability in the MPLS development." http://internetsociety.org/news/ietf-and-internet-society-statement-relating-today%E2%80%99s-itu-t-sg15-decision-will-lead-non

[99] For a detailed discussion of the IETF and its critics, see A. Michael Foomkin, "Habermas@discourse.net: Towards A Critical Theory of Cyberspace." Harvard Law Review Vol. 116 January 2003 Number 3. http://osaka.law.miami.edu/~froomkin/discourse/ils.pdf

Thus far these efforts have been largely unsuccessful. Standards organizations continue to churn out new and improved standards for the international market. However, there is concern that the situation could deteriorate. If governments become sufficiently frustrated with the way standards are being designed, or find that the existing standards process no longer serves their national economic or security interests, then we might see a large country like China, or a coalition of countries, decide to abandon the current standards process, effectively cleaving the Internet at the logical layer.

HOW ANARCHY WORKS[100] – THE INTERNET ENGINEERING TASK FORCE (IETF)

Much of that tension surrounding the standards arena revolves around the future of the Internet Engineering Task Force (IETF). The IETF is an association of researchers, academics and engineers, many of whom were instrumental in the early development of the Internet in the 1960s and 1970s. Since its founding in1986, the IETF has helped shape the majority of the Internet's core networking protocols (such as TCP/IP) and the protocols for the Internet's basic applications (e.g., SMTP for e-mail). The IETF is not the only standards body relevant to the Internet - there are literally dozens of other technical standards bodies that write and publish Internet-related standards[101] - but since the early days of the Internet it has been the body in which the most important standards needed for internetworking have been developed.

The IETF is an unusual standards organization among other standards groups. It calls itself a multistakeholder Internet standards organization – indicating that it seeks to represents a comprehensive set of interest groups with a stake in the standards process. But perhaps even more than other so-called multi-stakeholder organizations, the IETF seeks to be an inclusive, transparent, and intentionally (and unapologetically) non-hierarchical system of decision making.

The IETF also calls itself an open standards organization, in that membership in the IETF is open to anyone and all discussions and designs are publically available. Literally any individual who regularly participates in an IETF email mailing list or attends an IETF meeting can be said to be an IETF member.[102] Certainly, participation in the IETF decision-making process requires a strong technical understanding of the standard under development and its context, but IETF rules permit any person willing to contribute to participate. Further, decisions at the IETF are based on "rough consensus," a term left intentionally indefinite by the IETFs founding members, not majority voting. The IETF

[100] From a much read 1995 article from Wired Magazine by Paulina Borsook on the IETF, "How Anarchy Works." http://www.wired.com/ wired/archive/3.10/ietf.html

[101] The World Wide Web Consortium (W3C), the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and countless others also contribute to the standards process. However, for the purposes of this section, I will refer only to a small subset of these groups. The criticisms of IETF are also waged against other multi-stakeholder standards organizations, such as the W3C, albeit to a lesser extent.

[102] There is significant disagreement among scholars and standards professionals over what an open standards process is. The IETF definition is expansive. See: S. Bradner 1996 "The Internet Standards Process" http://tools.ietf.org/html/rfc2026#page-24; Berman Center Guide, "Roadman For Open ICT Ecosystems" http://www.apdip.net/resources/policies-legislation/guide/Berkman-Roadmap4OpenICTEcosystems.pdf

likes to boast that its rough consensus model streamlines decision-making in a way that more formalized majority decision-making cannot.

CRITICISMS OF THE IETF

It is undeniable that he IETF has been extraordinarily successful at producing technically sound standards over the years. Its standards tend to be more reliable, come to market faster, and are more readily adopted than those produced in competing standards bodies.[103] Yet despite its success at developing standards, the IETF is viewed with suspicion by a number of developing, as well as developed, nations around the world.[104] Beyond seeing the IETF as an anarchic institution with little oversight and few controls, critics suspect that the IETF is – as is the case with many multistakeholder institutions of Internet governance, like ICANN - simply an instrument of American political and commercial interests.

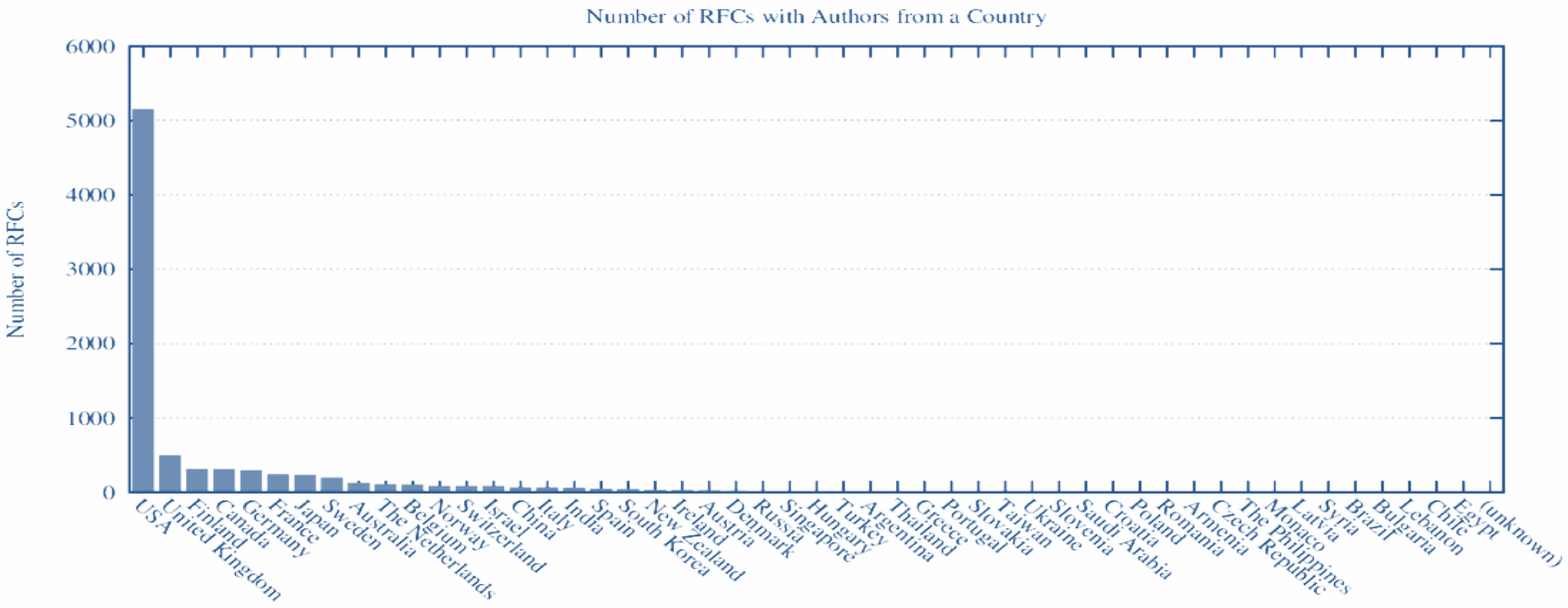
These critics stress the fact that Americans have dominated the IETF since its founding. Americans have held a disproportionate number of high-level positions within the organization, and American engineers have been responsible for the vast majority of the IETF's "Request for Comments (RFCs)"[105] documents, the technical peer-reviewed reports that often lead to standards. Of the more than 6000 RFCs drafted between 1986 and 2012, American engineers have drafted over seventy percent of them. Compare that number with the mere four percent of RFCs drafted by Chinese engineers, the two percent from India, and the less than one-half of one percent from Russia.[106] Granted, these RFC numbers date back to 1986, when the Internet was predominantly an American enterprise, but the pattern remains today: a more recent review of the RFCs reveal an IETF with a overwhelming American preponderance.[107]

This perceived American domination is more than an affront to the pride of non-American engineers; there is big money at stake. Although IETF standards are said to be "open," in that the process and technical specifications of the standard are available to the public, and although no central authority mandates the adoption IETF standards, most IETF standards contain within them patented technologies with licensing obligations due to the patent holder. As official policy, the IETF favors patent-free standards, but given the high cost of research and development for firms writing these standards patent free is often economically

[103] See Simcoe, Timothy. (2007) "Delay and De Jure Standardization: Exploring the Slowdown in Internet Standards Development" in Greenstein, Shane and Stango, Victor "Standards and Public Policy," Cambridge University Press.
[104] Interview, David Clark, MIT CSAIL Lab, December 2, 2011
[105] "Requests for Comments" The RFC series constitutes the IETF's primary body of work. Once developed, standards are published as RFCs, but other categories of work such as experimental protocols, informational documents, and proposed/draft standards are also included in the RFC series. RFC 1792, "Not All RFCs are Standards"; RFC 3160, "The Tao of the IETF."
[106] IETF Document Statistics "What's going on in the IETF?" http://www.arkko.com/tools/docstats
[107] Ibid.

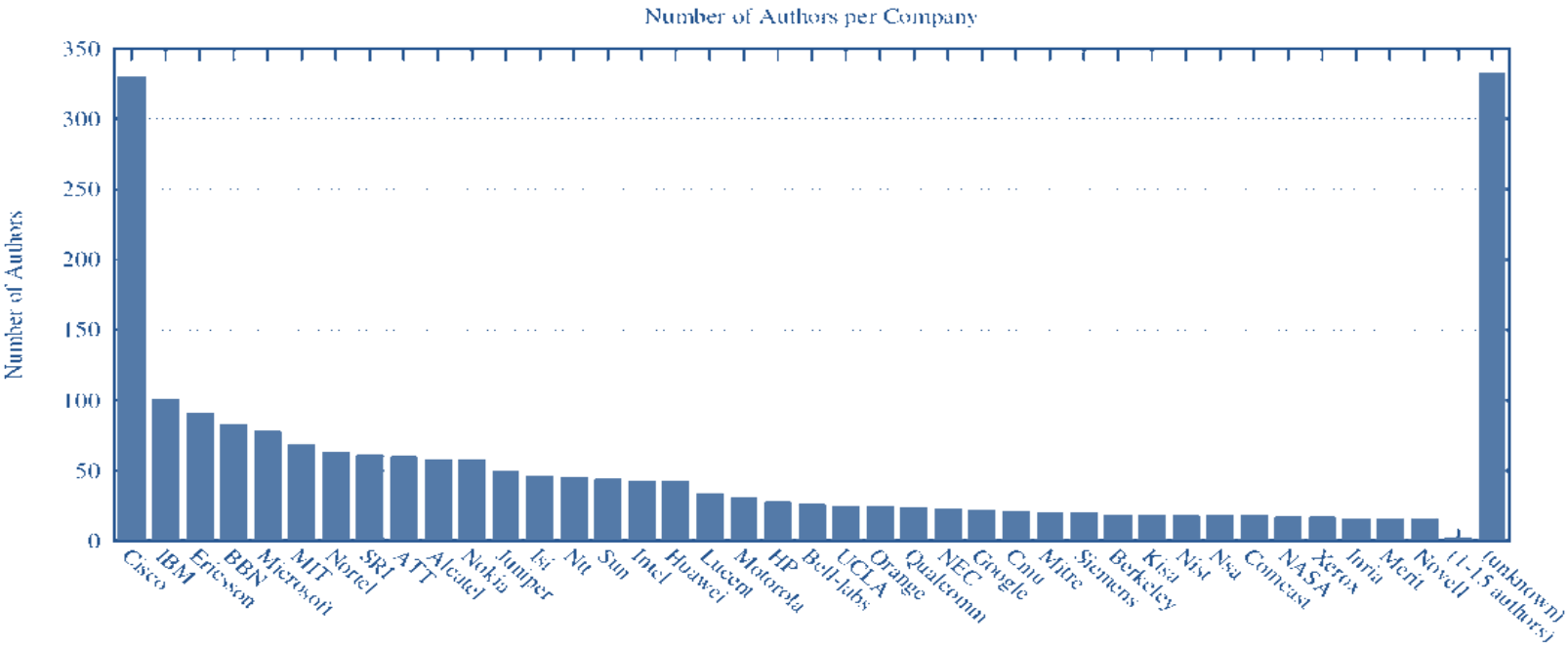
unfeasible.[108] With potentially billions of dollars at stake, one can see why non-American observers would be skeptical of a system that, in their eyes, favors American patent-holders.

A look at the number of RFCs on a firm-by-firm basis further validates critics' skepticism. From 1986, for instance, one American corporation, Cisco, has produced more RFCs than all of China's submissions combined. Huawei, China's largest ICT firm, is ranked a mere 17th in terms of RFCs and it is the only Chinese firm of the 40 top RFC drafters.[109]



Americans and IETF supporters argue that more American RFCs and more standards are adopted because they are the most technically sound standards. No government or firm is formally required to adopt an IETF standard; they do so because they are the best. But given the IETF's historical role as the Internet's core standards body, IETF standards have been the de facto standards for internetworking since the Internet's founding. Consequently, given the dominance of American engineers and firms at the IETF, and the vast amount of money exchanging hands in licensing fees, it is easy to see why non-American companies and governments might find the current status-quo IETF process unsustainable, even if the IETF is indeed advancing the most "technically sound" standards.

[108] Simcoe, Timothy. (2005) "Open Standards and Intelectual Property Rights." Open Innovation: Researching a New Paradigm (Oxford University Press), http://www.rotman.utoronto.ca/timothy.simcoe/papers/OpenStandards_IPR.pdf
[109] IETF Document Statistics, Ibid.



Many American engineers - and likely many of their non-American IETF colleagues – respond with the argument that American engineers are simply better trained and more experienced than their non-American colleagues.[110] The best research institutions are in the United States; the Internet itself was created under American auspices, they argue. Other countries' engineers are catching up technologically, but there is a lag time that has yet to be overcome. This argument may in fact be the correct explanation, but while American engineers may be better trained than their non-American counterparts, the numbers are still disproportionately weighted towards the Americans. The real reason American engineers have been so dominant at the IETF, the critics maintain, is that the IETF as an institution is fundamentally unreceptive to the participation of non-Americans, despite its attempts at (or claims of) radical inclusivity.

First, they argue that cultural barriers preclude non-Americans from equal participation in IETF discussions. All IETF meetings and email correspondences are conducted in English; English is the language of the all-important informal discussions that take place in the bars and hotel lobbies on the sidelines of the IETF meetings.[111]

Second, procedurally, the "rough consensus" model, the IETF self-proclaimed paradigm of inclusive decision-making, actually serves to give undue influence to incumbent engineers (read, Americans). Although everyone is free to participate in the IETF, it does not follow that every participant is equal. A member's reputation within the IETF often determines how seriously people take his or her opinion, and consequently in what direction the "rough consensus" of the group will go. Since these reputations and relationships take years to form, new entrants (read, non-Americans) who have not been present at the meetings since the early years, or who have not been present on the sidelines of the conferences at MIT or Cal Tech, not unrealistically perceives themselves as at a significant disadvantage. Thus as

[110] Berger, Arthur. Interview at Massachusetts Institute of Technology, November 1, 2011
[111] Clark, David. Interview at Massachusetts Institute of Technology, November 22, 2011

Baisheng An, former Deputy Director of the WTO Affairs Department of the Chinese Ministry of Commerce succinctly summarized, "If the United States currently claims more faithful adherence to international standards rules, those claims are only valid because those international rules were first and foremost designed by, and thus already in line with, the interests of the United States."[112]

STANDARDS CLASHES AND DEMANDS FOR CHANGE

In response to these real or perceived inequities, and the failure to influence the IETF in their favor, China, Russia, Brazil and India, among others, have attempted both to circumvent the standards process, and to take the de-facto standards production power entirely out of the hands of the IETF and to empower with ultimate authority over Internet standards the Telecommunication Union's Standardization Sector (ITU–T), or an entirely new UN multilateral organization.

Towards that end, as was mentioned above in the discussion of the DNS, the Indian government has formally called for the creation of an entirely new body, the Committee for Internet Related Policies (CIRP), to developing Internet policies, manage the DNS, and negotiate Internet related treaties, but also to oversee and manage all Internet standards bodies. Furthermore, in December 2012, at the renegotiation of 1988 International Telecommunications Regulations (ITRs) at the World Conference on Information Technology 2012 (WCIT-12) in Dubai, it is expected that Russia, China and perhaps other nations will propose a UN/ITU takeover of several areas of Internet governance, including Internet standards production.[113]

The ultimate effects of an ITU, UN or other multilateral takeover of the standards process is matter of debate. It is unclear exactly how the IETF, the World Wide Web Consortium (W3C) or any of the other major Internet standards organizations would function if either the India CIRP plan or the ITR renegotiation were to lead to a UN takeover. But it seems likely in either case they would continue to exist, but with the UN taking final authority over what standards were advanced.

The U.S., EU, Australia, Korea, Japan and Internet freedom advocates have responded vociferously to these proposals and are currently waging an international diplomatic campaign to have them rejected.[114] They worry that an ITU or a UN takeover of the standards process would mean a significant drop in the quality and speed of production of standards, and broader limitations on Internet freedoms.

---

112 Baisheng An. "Intellectual Property Rights in Information and Communications Technology Standardization: High Profile Disputes and Potential for Collaboration Between the United States and China." Texas International Law Journal, Vol. 45:175

113 Waz, Joe and Weiser, Phil. (2012) "Internet Governance at a Crossroads." http://www.huffingtonpost.com/joe-waz/internet-governance-at-a-_b_1203125.html

114 See FCC Commissioner Robert McDowell's 2012 Wall Street Journal article "The UN Threat to Internet Freedom" http://online.wsj.com/ article/SB10001424052970204792404577229074023195322.html; and Ambassador David Gross and Ethan Lucarelli "The 2012 World Conference on International Telecommunications: Another Brewing Storm Over Potential UN Regulation of the Internet" http://www. whoswholegal.com/news/features/article/29378/the-2012-world-conference-international-telecommunications-brewing-storm-potential-un-regulation-internet/

A SPLIT STANDARD?

What is generally overlooked in these discussions, however, is the question of what would happen if the status quo standards process were to continue unchanged. If China and others find that the IETF and the multistakeholder model of standards production continue to be unacceptable, what would they do? Might China or a coalition of countries unilaterally pull out from the IETF process by mandating the adoption of non-IETF standards? It has happened before.

In 2003, for example, the Chinese government mandated a Chinese-designed alternative to the WiFi wireless family of protocols designed by the Institute of Electrical and Electronics Engineers (IEEE)[115] called the WLAN Authentication and Privacy Structure (WAPI). The Chinese government argued that the international IEEE standard for WiFi had serious security flaws and that it required the payment such high royalties that it was damaging domestic Chinese firms. In order to promote the Chinese WAPI standard, the Chinese government set a requirement that all new devices in China using wireless technologies would have to include WAPI configurations. This break from the international standard posed a serious problem for non-Chinese vendors who, under the particularly protectionist terms of the WAPI requirement, would have been unable to reach the Chinese market. It was only under high-level pressure from the U.S. government and the threat of WTO intervention did China ultimately suspend its WAPI requirement – although the issue remains under discussion in the Internet Organization for Standardization.[116]

While the WAPI case did not pose a risk to the Internet's networking protocols and only impacted those devices in China using wireless technology, the WAPI case is nonetheless illustrative of the type of standards policy China, or perhaps a coalition of countries including China, could pursue if their concerns are not addressed. Governments could mandate that all domestic vendors configure their equipment to run on non-IETF standards; in a more extreme situation, governments could even place an outright ban on IETF standards altogether.

Given its large consumer market, growing self-confidence, and desire to advance domestic technologies, China would likely take the lead in any standards cleavage. But other countries, similarly dissatisfied with the IETF, or hoping to move closer economically or politically to China, might follow suit. Such a move by China or a coalition of countries might not cleave the Internet in a dramatic way, and lead only to a more expensive market for Internet products. But it also could, depending on the type of standard and the way the laws and regulations were written, significantly affect the interoperability of the Internet.[117]

---

[115] The IEEE is responsible for a number of telecommunication standards, which, like the IETF is a majority American-member organization More than fifty percent of the IEEE's members are from the US, see: http://www.ieee.org/about/today/at_a_glance.html#sect1

[116] For an excellent overview of the WAPI case, see: Baisheng An. Ibid

[117] A useful case study is the split that occurred between the MPLS and T-MPLS standards. As a result of IETF/ITU failed coordination, and Chinese industry lobbying efforts, the ITU advanced an un-interoperable version of an IETF standard. For a good overview, see "ITU bellheads and IETF netheads clash over transport networks" http://arstechnica.com/tech-policy/news/2011/03/itu-bellheads-and-ietf-netheads-clash-over-mpls-tp.ars; and the comment by the Internet Society, http://internetsociety.org/news/ietf-and-internet-society-statement-relating-today%E2%80%99s-itu-t-sg15-decision-will-lead-non

HOLDING THE INTERNET TOGETHER THROUGH STANDARDS

Today, Western governments, particularly the United States, are waging a concerted diplomatic campaign to keep the Internet free from the type of UN government control proposed by India through the CIRP, or China and Russia through the ITRs. The US and others have tried to make the case that such a move would, among other things, significantly limit the Internet's ability to grow and innovate.

What is being left out of these discussions, however, is how the real or perceived grievances of non-Western nations can be met if the current system continues. If the US wishes to ensure a continuing cooperative standards process, it will need to initiate a renewed effort to address the concerns of those countries which view themselves as at a disadvantage in the current standards process. At the same time, those who support the IETF and the current standards process should strive to inform ("to lobby" might be a more honest verb) responsible persons and agencies from those countries presently on the fence, about the very real threat to a unified (and productive) Internet posed by those who favor balkanized standards. As Phil Weiser recently wrote, "To take the traditional model of Internet [standards development] for granted would be a grave mistake. Protecting and developing this model will take considerable work and direct engagement by stakeholders, at the WCIT in Dubai and elsewhere."[118]

[118] Waz, Joe and Weiser, Phil. (2012) "Internet Governance at a Crossroads." http://www.huffingtonpost.com/joe-waz/internet-governance-at-a-_b_1203125.html

VII: Fragmentation at the People Layer: Localized Privacy Requirements

"Building a single European data protection regime is hard enough. Harmonizing it with America will be harder. Reaching deals with Indian bureaucrats and Chinese mandarins set to defend the interests and the data of their countries' rapidly growing online firms may be downright impossible."
The Economist[119]

PROTECTING PRIVACY THROUGH REGULATION

The Internet allows for the rapid and inexpensive collection of vast amounts of personal information and data online. Internet companies and ISPs collect users' information through searches, purchases, sign-ins, and HTTP cookies, and then use that information for any number of purposes, from improved search engine results to better-targeted advertising. But while the collection of personal information and data has generated billions of dollars of online revenue and spawned new industries,[120] privacy advocates around the world are up in arms about the collection and use of this data, and what they view as a mounting threat to personal privacy and a lack of serious online consumer protections.

In response to these concerns, governments are crafting new rules addressing how digital data are collected, stored and sold. Whether privacy protections should be enforced through legislation, or through voluntarily measures by Internet companies, is a matter of intense debate. But if the recent wave of new proposed privacy rules in the U.S. and internationally is any indication, the tide of public and government opinion seems to be shifting towards increased legal protections for Internet users and their personal information.

Hidden within these privacy deliberations, however, lies a real threat to the Internet's unity. Amidst the flurry of new privacy legislation under discussion in world capitals, there has been remarkably little international coordination or agreement about what types of restrictions and limitations should be put on the acquisition and use of online data. There

[119] "Private Data, Public Rules" January 28, 2012 http://www.economist.com/node/21543489
[120] A Booz and Co. study estimates that the ad-supported Internet generates roughly $100 billion of consumer surplus each year in Europe and the United States. http://www.booz.com/media/uploads/BoozCo-Impact-EU-Internet-Privacy-Regulations-Early-Stage-Investment. pdf; and according to the Interactive Advertising Bureau, digital advertising revenues in the United States were $7.88 billion for the third quarter of 2011, a 22 percent increase over the same period in 2010. http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=1&ref=technology&src=me

are mounting concerns that if many countries adopt their own unique privacy requirements, then every firm operating on the Internet could potentially be subjected to a multiplicity of often inconsistent laws. If companies are unable to meet each country's differing requirements, either because those requirements are in conflict with one another or because of the added costs associated with meeting multiple disparate rules, then we could see firms pulling out of particular markets entirely, essentially balkanizing the Internet by firm.

WORLDWIDE EFFORTS

Across the world, governments are proposing and promulgating new rules and setting new codes of conduct to protect user information online. In the United States, lawmakers have historically relied largely on industry self-regulation rather than statutes and regulations, in line with traditionally American laissez-faire principles and the long-argued assertion among industry leaders that regulations are a hindrance to technical innovation. As a result, there are today few United States laws governing how personal information is collected, stored, or sold online. But as the Internet has moved into a new era of growth, fueled by new and emerging technologies—including widespread broadband access, cloud computing, social media, and mobile connectivity—new protections are increasingly likely to come from Washington.

In Congress, a number of bills have been introduced, including the Speier "Do Not Track Bill" (H.R. 654), the Rockefeller "Federal Do Not Track Bill" (S. 913), the Kerry-McCain "Federal Privacy Bill" (S. 799), and the Stearns-Matheson "Federal Privacy Bill (H.R. 1528), among others. The Administration too has been active, with the White House having outlined a series of online consumer privacy "principles"[121] to guide industry privacy polices. The Federal Trade Commission (FTC), likewise, has released "Protecting Consumer Privacy in an Era of Rapid Change" in December 2010,[122] with similar goals in mind. All these efforts are, in one way or another, attempts to satisfy consumer privacy concerns while not stifling the growth of online advertising, which is seen as a potential savior of media and publishing companies as well as a boon to the advertising industry in particular and the economy in general.

Outside of the United States, governments are proposing far more restrictive rules than have been contemplated by Americans. In China, for instance, the Ministry of Industry and Information Technology recently issued draft rules on data protection rules (inelegantly translated as the "Several Provisions on Regulating Market Orders of Internet Information Services," or, the "New Regulations")[123] that, when they go into effect in March 2012, will severely limit the ability of commercial organizations to collect and transfer personal data. ISPs and other firms will be required expressly to inform Internet users of the method, content, and purpose of collecting and processing personal information, and will be prohibited from collecting any information that is not necessary for their services.

---

[121] Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

[122] FTC Privacy Report, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[123] The New Regulations (in Chinese) http://www.miit.gov.cn/n11293472/n11293832/n12843926/n13917012/14414975.html

In India, similarly, the Ministry of Personnel, Public Grievances and Pensions has recently released a new draft of its "Reasonable Security Practices and Procedures and Sensitive Personal Information Rules," otherwise known as the "Right to Privacy Bill,"[124] an update to India's 2008 IT Security Act amendment. The bill defines both "personal information" and "sensitive personal information" and prescribes how such information may be collected and used by virtually all organizations in India. The new rules would give India's courts incredibly broad powers to control information online. However, the rules are not as clear as one might wish. The rules state that,

> *"Every individual shall have a right to his privacy — confidentiality of communication made to, or, by him — including his personal correspondence, telephone conversations, telegraph messages, postal, electronic mail and other modes of communication; confidentiality of his private or his family life; protection of his honour and good name; protection from search, detention or exposure of lawful communication between and among individuals; privacy from surveillance; confidentiality of his banking and financial transactions, medical and legal information and protection of data relating to the individual."*

Because of significant ambiguity found in the language of the bill, the relevant authorities in India will surely have to issue further regulatory clarification so that both the courts and regulated companies will know what, on a practical level, is permitted and what is prohibited. But even prior to clarification, it is certain that the applicability of the rules is very broad: they appear to apply to all information in the possession of organizations in India, regardless of from where the information came or how it found its way to India. It seems clear that if these new rules are enforced as written, they could have a profound effect on multinational businesses that either outsource business functions to Indian service providers or maintain their own operations in India.

Internet privacy concerns are finding their way into legislation in Europe as well. The European Commission announced on January 25, 2012, that it was instituting a comprehensive set of reforms to the EU's online data protection regime, an update to the severely outdated Data Protection Directive of 1995.[125] If implemented as proposed, the proposed EU privacy rules would represent perhaps the strictest and most sweeping privacy regime in the world.[126] The new rules would require that companies obtain "specific, informed, and explicit consent" from individuals in order to use personal data collected online. Furthermore, they would force online firms to justify any information they collect, and would allow the firms to keep that information in their systems only so long "as it is needed." The new regime would also give Internet users the legal right to demand that firms

[124] For the text of the bill, see http://cis-india.org/internet-governance/privacy-matters-analyzing-the-right-to-privacy-bill/draft-bill-on-right-to-privacy

[125] For the complete 1995 Directive, see: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

[126] "Microsoft, Google Groups Warn EU on Overly Strict Privacy Rules" http://www.bloomberg.com/news/2011-11-28/microsoft-google-groups-warn-eu-on-overly-strict-privacy-rules.html

holding their personal information erase all their data stored online, a "right to be forgotten."[127]

The Commission maintains that the new rules will not only strengthen online privacy protections for EU citizens, but will bring much needed uniformity to the many different - and thus often inconsistent - privacy requirements of the individual EU member states. A firm based anywhere in Europe should now be able to comply with both domestic law and do business across the EU, without having to worry about whether its actions satisfied each of the 27 individual member states' domestic regulations. Any company failing to comply with these new regulations would incur severe penalties – as high as two percent of a company's global revenue[128] - sanctions enforced by a newly created European Data Protection Board.[129] It is an irony of Internet regulation that this European Commission effort to unify privacy rules (and thus to avoid a multiplicity of local European regulations) may result in Europe diverging from North American privacy approaches.

A CLASH OF POLICIES

All of these new government efforts at privacy protection, whether in the United States, China, India, the EU or elsewhere, seek at least in theory and rhetoric to protect consumers from abuse or unauthorized use of their personal data. Yet increased government privacy protections - legitimate as they may be – nevertheless hold the potential for serious, if unintended, fragmentation of the Internet.

When different countries enforce dramatically different rules with regard to how and where data can be collected and stored, when and under what conditions data be transferred to other organizations, and what types of user authorizations are needed for collection, storage and transfer, international Internet firms are put into a very difficult situation. Firms must either adjust their internal data collection, storage and transfer methods to meet the standards of every unique system - which may stretch from technically challenging to outright impossibility – or try to skirt the law and perhaps face constant litigation and corresponding burdensome sanctions. By either strategy, compliance or evasion, companies will be faced with tremendous logistical problems and enormous expenses.

Differences between privacy regimes are not new. The EU and the U.S., for instance, have long enforced divergent privacy requirements for online firms. Under the 1995 EU Privacy Directive, organizations could only transfer personally identifiable information from the EU to countries that the European Commission had deemed to have adequate data protection laws – the U.S. was not one of those countries.[130] In order to mitigate the effects of these

[127] Critics warn that removing a users data from all systems can be an extraordinarily complicated process. Data does not always stay in one place; if it is transferred to another company, say for analysis and market research, it cannot easily be recollected and deleted.
[128] "Europe Weighs Tough Law on Online Privacy" http://www.nytimes.com/2012/01/24/technology/europe-weighs-a-tough-law-on-online-privacy-and-user-data.html?pagewanted=all
[129] "Commission proposes a comprehensive reform of the data protection rules" http://ec.europa.eu/justice/newsroom/data-protection/ news/120125_en.htm
[130] See Thompson, Mozelle. FTC Commissioner. (2003) "About the Future of Cross Border Data Proection." http://www.ftc.gov/speeches/thompson/thompsonsafeharbor.pdf

differences in the past, in 2001 the U.S. and EU agreed to a safe harbor approach by which American companies, working under less-demanding domestic U.S. laws, and European companies sending data to the U.S., were both safe from European litigation as long as they adhered to certain basic privacy principles set forth the 1995 EU directive.[131] With the EU's more stringent privacy rules coming into effect, however, the safe harbor agreement may no longer hold, especially given the languor with which privacy legislation is moving through the U.S. Congress.

In the meantime, European regulatory pressure is building on some American firms. Google is one firm which has come under increased scrutiny in regard to its own new privacy policy, having already been notified by the France's data privacy regulator, the Commission Nationale de L'Informatique et des Libertes (CNIL), that the company's new privacy policy will likely not meet the requirements of the update to the 1995 directive.[132] Facebook too is concerned that the new EU rules will threaten its business; it has been making a concerted effort to demonstrate how much the EU's digital economy could be hurt if it (as well as companies that use Facebook as a business hub) is forced to change its business model.[133]

Similar concerns are being voiced about Chinese and Indian regulations. Observers point out that Chinese Internet regulations have often been arbitrarily or selectively enforced. They note as well that India's requirement that individuals' "honour and good name" be protected creates an extraordinarily overbroad legal standard, making compliance uncertain and enforcement arbitrary. For American and other foreign firms, this is particularly troubling, since the law would undoubtedly apply to Indian citizens working for outsourcing operations of multinational corporations.

A MARKETPLACE DIVIDED

If the recent problems in the EU encountered by Google and Facebook are illustrative of what is to come, it will probably be the largest and most prominent companies that will come underthe most legal scrutiny. However, while these large companies may suffer the greatest public pressure, it is likely that smaller companies, particularly those that are just developing their technologies and markets, may be the most adversely affected, since they may not have the technical ability, the legal counseling, or the financial resources necessary to operate across jurisdictional borders—and if necessary, to litigate in many courts. These businesses (many of whom may comprise the future of the Internet) could decide – or be forced – to pursue business in certain countries only.

---

[131] United States Trade Representative, "A Guide to Self-Certification; U.S. EU Safe Harbor Framework" http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf; For an overview of the Safe Harbor requirements, see http://export.gov/safeharbor/eu/eg_main_018476.asp

[132] "Google's New Privacy Policy May Violate E.U. Rules" http://www.nytimes.com/aponline/2012/02/28/business/AP-EU-Google-Data-Privacy.html?_r=1&ref=technology

[133] "Facebook's Sandberg Gently Warns Europe About Privacy Rules" http://bits.blogs.nytimes.com/2012/01/24/facebooks-sandberg-gently-warns-europe-about-privacy-rules/

But even larger companies, such as Facebook and Google, which do have the economic and technological capacity to deal with differing local rules, may elect to withdraw from certain countries if they conclude that compliance with multiple regulatory regimes is overly demanding, or the benefits of operating in those countries do not justify the demands in terms of money and corporate energy.

The result of large and small companies opting out of various nations would be to deny access to users from those nations; to divide companies along national lines, and nations along company lines. Surely, if this occurs, the Internet as encountered in one country will differ dramatically from the Internet found in others. This unintended consequence of otherwise sound and appropriate privacy concerns could thus dramatically shift the Internet to the right of the Fragmentation Spectrum.

VIII: Conclusion

	Layers Affected	Actors and Forces	Balkanization Potential
IPv4/IPv6	Logical	National Governments, Technological Changes, ISPs	Low – Some loss of application
DNS Split Root	Logical	National Governments/ International Organizations (ICANN)	Strong – Potential loss of interoperable DNS
Filtering/Blocking	People, Information, Logical, Physical	National Governments, ISPs	Strong – Websites, applications and content restricted
Pricing Schemes	People	ISPs, Backbone providers, Government regulators	Low – Unlikely to affect access.
Standards	Logical, People	International Organizations (IETF,ITU,SSO), National Governments, Business Interests	Low to Strong – Depending on which standards are split.
Privacy Laws	People, Information	Users, National Governments	Medium – depending on the types of laws.

(Summary Table)

As I hope this paper demonstrates, these six separate threats to the interoperability and global reach of the Internet are all immediate and, unless addressed by the international community, potentially devastating to the future that most stakeholders in the Internet would surely wish: a seamless system by which all users may exchange information freely, and engage in commerce with all others on the network. Yet some stakeholders, especially national governments and certain commercial interests, are pressing for changes in the Internet and its governance structure that, while undoubtedly thought to be consistent with their national or corporate interests, may result in a significant deterioration of the Internet's global reach and impact.

The conclusions drawn from this analysis of those threats are, lamentably, not sanguine because there are now so many distinct forces and interests creating and multiplying the threats. Given that in the coming years there will surely be a dramatic series of changes as profound, if not more profound, than those witnessed over the past two decades, it would seem inevitable that the challenges of balkanization will continue, and take on new and unanticipated forms. The United States government must step up its efforts to address each of these problems if irreparable balkanization is to be avoided.

Looking at the summary chart above that demonstrates the diversity of the issues and the actors and forces driving the six threats, it is evident that policymakers will need to employ an equally diverse and innovate array of policy tools to keep the Internet together. To begin, rigorous bi-lateral and multilateral diplomacy and outreach will be essential to persuade governments and non-governmental entities to take necessary action to mitigate the threats.

Certainly, some of the six identified threats will be more challenging to remediate than others. In particular, those threats the solutions for which are primarily technical in nature, such as the transition to IPv6 or net-neutrality, will in all likelihood be more easily remedied then those issues, such as censorship and privacy, which are more deeply rooted in culture and politics. Indeed, in the case of online censorship it could be argued that governments are deliberately pursuing policies that are having the effect of fragmenting the Internet. Technical issues may require expensive and sophisticated engineering solutions, but policy makers may find that a change in technical policy will be far less intractable than changes which require states to dramatically alter or abandon longstanding ideological positions and notions of national sovereignty and security.

Accordingly, one central policy objective of the United States must be to develop a convincing case to governments around the world that full participation in the global Internet is, despite its risks, preferable to isolation. Secretary of State Clinton's 2010[134] and 2011[135] speeches on Internet freedom were a laudable start, but they were only a start. U.S. policy-makers need to provide real, actionable evidence of the value of an interoperable Internet, as well as a compelling case why a unified internet is in every country's national interest, not just that of the United States. To make this case to authoritarian governments will require especially sensitive and subtle diplomacy, because the case to them will have to address, to no little extent, their national security concerns—concerns that, for ideological and cultural reasons, the United States does not share.

Certainly, no diplomatic effort will be more challenging, or more important, than that directed to China. More than any other country, China - as a result of its enormous population, growing economic clout, increasing international political assertiveness, and concern for its own internal political stability – will not easily be deterred from acting, with respect to the Internet, in what it perceives to be its national interests. Not only is it a great power not easily susceptible to American advise, but precisely because of its size, wealth and international influence, China is less likely to be deterred by alarms concerning the risks of isolation. In nearly all of the six case studies explored above, China has played a central, if not the central role in pushing the Internet to the right of the fragmentation spectrum. It was the only country fully to operationalize its own unique DNS root; it was the only country effectively to deviate from international technical standard regimes; and it has developed the world's most sophisticated censorship regime.

In light of these actions, it is arguable that Chinese government understands precisely where its policies may be leading, but believes that the nation is sufficiently great in population, wealth and influence that it cannot be isolated in a way that would do it profound harm. Accordingly, American policy-makers must treat China as a special case, and expend the necessary political capital and resources to persuade the Chinese government and its people that the threats to their future is greater than the threat presented by an interoperable Internet.

---

[134] Clinton, Hillary. (2010) "Remarks on Internet Freedom"
http://www.state.gov/secretary/rm/2010/01/135519.htm

[135] Clinton, Hillary. (2011) "Internet Rights and Wrongs: Choices and Challenges in the Networked World"
http://www.state.gov/secretary/rm/2011/02/156619.htm

However, beyond government-to-government outreach, the United States must also continue to make the case against Internet fragmentation (in all its forms) with the private sector. Furthermore, in an expression of non-traditional diplomacy, the United States should make the case to the world's general public, which may not realize the risks it faces.

Finally, the discourse concerning Internet balkanization and fragmentation in Washington and around the globe needs to change, and expand to critique not only government efforts to separate their citizens from the wider Net, but also those technical and cultural barriers that keep people separated on the Internet. Not all barriers to a free Internet are the construction of authoritarian governments, and thus the conduct of those governments, unhelpful as they are, should not be the sole topic of our government's conversation in this regard. The United States must align itself against all material barriers, even (perhaps especially) those put in place by American companies. Our policy must recognize the complex array of challenges to the unified Internet, and make the case in every quarter that Internet barriers can have effects much like real walls and borders that divide societies. When barriers are erected, it becomes much more difficult to maintain accord among societies and peoples; when they come down, the lives of the citizenry are enormously enriched.

About the Author

Jonah Force Hill is a third-year graduate student pursuing dual-masters degrees at Harvard Divinity School and the Harvard Kennedy School of Government, where he is a Belfer Center for Science and International Affairs Fellow. At Harvard, Jonah has served as the teaching fellow for the course, "International Cybersecurity: Public and Private Sector Challenges" and as the Program Assistant for the Belfer Center's India and South Asia Program, among other research positions. Prior to his graduate studies, Jonah worked with the U.S. Department of State at the U.S. Embassy in New Delhi and the U.S. Consulate in Mumbai, and spent the summer of 2011 working in the Office of the Cybersecurity Coordinator at the White House.

Jonah can be reached at jonahforcehill@gmail.com