CS 978 – Legal, Ethical, and Professional Issues for the Information Society

University of Strathclyde Glasgow

Week 1– Internet governance

Introduction

While almost all of us use the Internet on a daily basis, there is an arguably limited understanding within mainstream society of how the Internet is actually governed. This week we will discuss some of the issues around Internet governance, and the challenges that may be raised for the future.

The nature of Internet governance

The success of the Internet has been unprecedented in human history. In December 1995 the Internet had 16 million users, and by June 2015 the estimate for users was 3.2 billion across the globe. Yet arguably with its explosion in usage and impact the original goals of the medium have been under pressure.

In 1996 the manifesto that overarched the early days of the Internet was published by J.P. Barlow. You can read the full text via the link below, but some snippets reveal how the early Internet pioneers saw the medium:

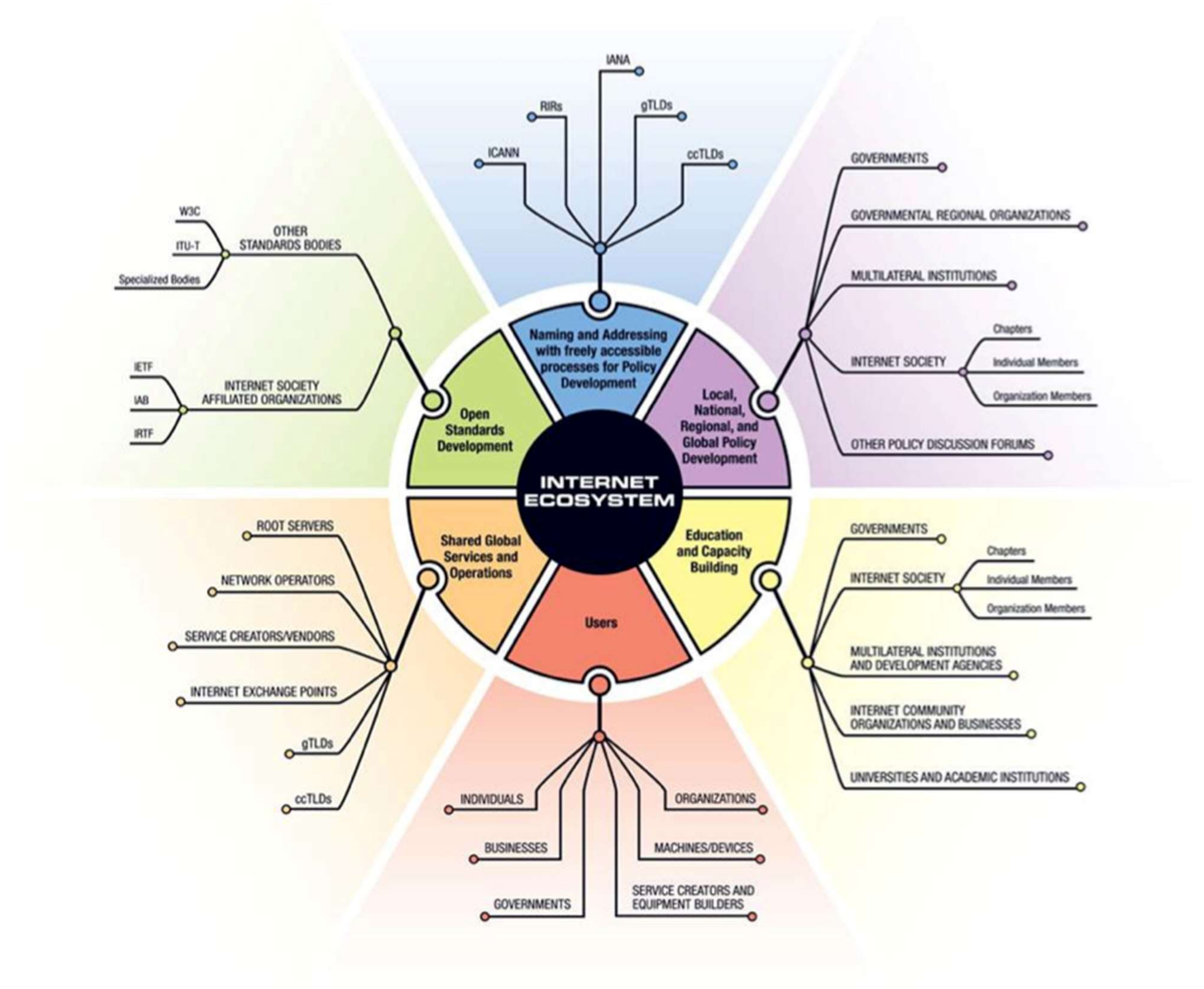
> "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." [1]

Whether such grand notions for the medium were ever truly real, there was certainly a feeling among early adopters and those who shaped the Internet that this was an entirely new paradigm shift in humanity, and one that would be free of governmental and commercial influences. As Lessig states, "The claim for cyberspace was not just that government would not regulate cyberspace—it was that government could not regulate cyberspace." [2]

The Internet is governed in a multi-structured way, with several organisations responsible for separate aspects of it. These groups include the Engineering Task Force (IETF) and the Internet Architecture Board (IAB), as well as the Internet Society (ISOC). The mission and mandate of the Internet Society are focused on the education, empowerment and awareness of governments, businesses and the users around the world. The Internet ecosystem is described in the following image (the PDF of the image and an explanation of the organisations is on MyPlace):

[1] Barlow, J.P. *A Declaration of the Independence of Cyberspace*. https://projects.eff.org/~barlow/Declaration-Final.html

[2] Lessig, Lawrence. *Code version 2.0* (p. 3). Kindle Edition


INTERNET ECOSYSTEM
Naming and Addressing with freely accessible processes for Policy Development
IANA
RIRs
gTLDs
ICANN
ccTLDs
Local, National, Regional, and Global Policy Development
GOVERNMENTS
GOVERNMENTAL REGIONAL ORGANIZATIONS
MULTILATERAL INSTITUTIONS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
OTHER POLICY DISCUSSION FORUMS
Education and Capacity Building
GOVERNMENTS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
MULTILATERAL INSTITUTIONS AND DEVELOPMENT AGENCIES
INTERNET COMMUNITY ORGANIZATIONS AND BUSINESSES
UNIVERSITIES AND ACADEMIC INSTITUTIONS
Users
INDIVIDUALS
BUSINESSES
GOVERNMENTS
ORGANIZATIONS
MACHINES/DEVICES
SERVICE CREATORS AND EQUIPMENT BUILDERS
Shared Global Services and Operations
ROOT SERVERS
NETWORK OPERATORS
SERVICE CREATORS/VENDORS
INTERNET EXCHANGE POINTS
gTLDs
ccTLDs
Open Standards Development
OTHER STANDARDS BODIES
W3C
ITU-T
Specialized Bodies
INTERNET SOCIETY AFFILIATED ORGANIZATIONS
IETF
IAB
IRTF

The ecosystem of the Internet provides a unique governance structure of a type that was originally designed to make the medium as participative and open as is possible.

Code is law

An important concept around Internet governance is the idea proposed by Lawrence Lessig that *code is law*. A unique aspect of the Internet medium was that it was a system designed around computer code and systems architecture. This meant that those very things could be used to govern interactions with the system. Every act performed on the Internet involves the use of code and a systems architecture to achieve the desired result, and that meant those things could be used to control the experience. This clearly gave this writing the code and designing and managing the infrastructure immense power to shape the Internet experience. Lessig argues that:

> “the invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. This invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly efficient regulation possible. The struggle in that world will not be governments. It will

> be to assure that essential liberty are preserved in this environment of perfect control." [3]

In terms of code being law, Lessig clarifies his argument and the importance of that idea: "In cyberspace we must understand how a different "code" regulates— how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is, also regulate cyberspace as it is." [4]

Governance concerns

Cerf et al have observed that despite the desire of many that the internet remains an open and universal experience "over the last several years more and more governments and companies have been taking action to control the flow of information over the Internet" [5] As we will see below, this focus on the influence of governments and companies forms a significant tranche of the concerns over what has been called, *internet fragmentation*.

In his testimony on the future of the web to the US House of Representatives, Tim Berners-Lee identified three internet concepts that he argued were crucial to the foundation of the web:

1. Universal linking
2. An open foundation for information-driven innovation
3. Separation of layers [6]

Hill mirrors this analysis more broadly and argues that:

> 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. [7]

These ideas are potentially under challenge as the internet evolves, with arguments that both the openness and the freedom from government intervention of the ideal internet experience are under threat.

Although Berners-Lee was talking specifically about the web, as one would expect given his role in its evolution, he is clear that the values that underpin the internet made the web a reality. Hill cites Berners-Lee again expressing his view that the laws of the internet should be akin to the laws of physics; namely that the laws that apply in one area of the internet should apply everywhere on the internet. [8] The emphasis here, then, is on the internet where every netizen can be assured of sharing a universal experience. Hill contrasts this with what he believes is the developing fragmented internet and posits that there is a "fragmentation spectrum" with Berners-Lee's concept of the universal experience at one end, and an experience that is arbitrary, depending on location, at the other. The figure is represented below (*please note the misspelling of Berners-Lee's name is Hill's*):

[3] *Ibid* (p.4).

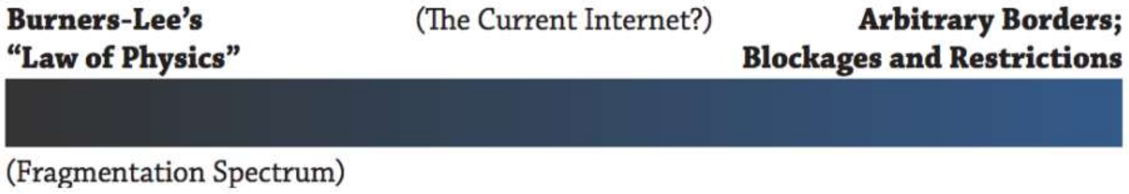
[4] *Ibid* (p.5)

[5] Cerf et al. 10 ISJLP 1 2014 p.2

[6] Berners-Lee, T. *The Future of the Web.*

[7] Hill, *Op. cit.* p.14

[8] *Ibid*. p.11-12



Hill acknowledges that it is difficult to place where on the spectrum the current internet experience is, however, he cites several elements as dangers netizens need to be aware of less the placement on it is not to be towards the more reductive experience.

You can consult Hill's report to gauge the issues he raises, and we will consider three of them in this week's lecture. As we will see, the concerns encompass several areas that incorporate fears of both technical issues, and policy/regulation issues.

Peering and Transit Agreements/Net Neutrality

The concept of *net neutrality* is perhaps one of the most progressive elements of the original pioneers of the internet. Net neutrality is built around the idea that regardless of the source, internet service providers (ISPs) should provide access to all content without fear or favour, and it is a truly admirable one. Increasingly net neutrality has arguably been under pressure as commercial concerns seek to cloud out traditional internet values. The increasing tendency for ISPs to offer valued-added services from partners related to their content runs the risk that they will favour this content over other content when providing services to their customers.

Net neutrality is of vital importance in terms of keeping the internet running smoothly. As French notes, while the internet has evolved into bandwidth-hungry services that rely on quick and efficient packet switching to ensure the service is provided (i.e. online gambling, skyping, video streaming), the internet was not originally designed for this, nor was net neutrality as a concept built around the reality of the internet that offered such services. Therefore the infrastructure has had to deal with highly increased capacity and had to undergo essential and expensive improvements in bandwidth capability.[9]

One solution is to more heavily regulate how ISPs offer their services, ensuring they commit to providing a steady service for all. The concerns expressed by those who advocate tighter regulation are highlighted by McCartney, namely the fears that "dominant broadband providers, such as AT&T and Comcast, will use their market power in consumer markets unfairly, favouring Internet content in which they have a financial interest." [10]

French argues that essentially three concepts underpin the net neutrality debate, namely freedom of expression, consumer protection, and innovation and economic growth. [11] Freedom of expression is limited if ISPs are able to throttle content from a service they do not favour. While the intention may not be to censor, the favouring is strictly business, the end result is that legitimate content is not seen by internet users. A recent example of this was highlighted on BBC News where T-Mobile was argued to be favouring its own video streaming service, Binge On, across its US network while throttling content from providers such as Youtube. [12] The Binge On service provided content from T Mobile's partner Netflix at the expense of other providers.

[9] French, T. (2007) 4:1 &2 UOLTJ 109. p.115

[10] 64 Fed. Comm. L.J. 493 2011-2012. p.494

[11] French. *Op. cit.* p.116

[12] see "t-mobile 'breaks' net neutrality rules with binge on" http://www.bbc.co.uk/news/technology-35232288

The second of French's concepts, consumer protection, is also of vital importance. When a consumer signs up for an ISP account, they are reliant on the service that the ISP provides. They have little way of knowing unless they are informed netizens aware of issues such as net neutrality, whether the reason they cannot access a service is because the service provider is poor, or the ISP is merely throttling bandwidth. Given it is unlikely that a consumer would be able to cite throttling as a reason for getting out of an ISP contract, we have an added element of concern re consumer protection.

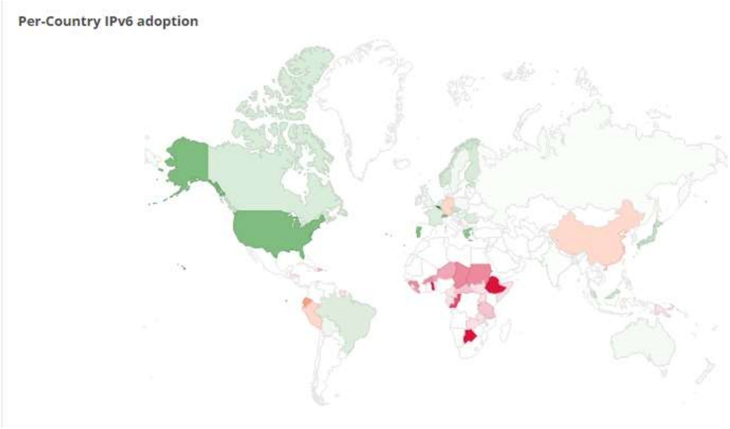
Lastly, innovation and economic growth are stifled if ISPs are allowed to favour content from one provider over another. The investment a company may put into providing an excellent service may well be wasted if consumers cannot access it efficiently. If the reason they cannot do so is, again, throttling of content, then a company is having its commercial interests restricted by another with vested interests. This not only goes against the values of the internet, it is also arguably anti-business generally, and risks stifling innovation and creating monopolies. We can see then that net neutrality does indeed raise issues with regards internet fragmentation that we must be aware of.

The Piecemeal Transition from IPv4 to IPv6

A technical concern relates to the very low take-up of IPv6 from the inferior and almost exhausted IPv4. IPv4 has coped manfully with the emerging internet, however, as a system conceived of in the 1970s when the concept of multiple devices with individual IP addresses not even dreamt of, the system was quickly running out of addresses. In actual terms, IPv4 allowed for up to 4 billion internet addresses. IPv6, on the other hand, allowed for 340 trillion, trillion addresses. In an era where even devices like watches and refrigerators require IP addresses, the new protocol was seen as an essential innovation.

What is the reality re IPv6, then, and why does it matter? According to the Internet Society, IP addresses on the IPv4 protocol will run out within a year. In theory, this means that no new numbers can be allocated and that anyone looking to add new devices to the internet will not be able to obtain one. However, this is not as clearly a doomsday issue as it might seem, since there is a trade in IPv4 addresses from organisations who own addresses allocated to them that they do not use. This trade is perhaps why IPv6 adoption has not been the pressing concern for many organisations that technologists may wish it to be.

Google provides a useful set of data on IPv6 adoption since it was launched, and if we consider the issue of internet fragmentation from an adoption perspective, we can see clear differences in the experiences and extent of adoption. As of 13th December 2015, 9.91% of the traffic to Google was using IPv6. [13]



[13] Google IPv6 statistic. https://www.google.com/intl/en/ipv6/statistics.html

The green areas of the map indicate high take up and satisfactory experience of adoption, whereas the red and pink areas indicate low adoption and reliability with those servers running it. If a picture could say a thousand words it would say that IPv6 adoption is fragmented, and three years on since its launch much more work needs to take place on its growth. Significantly one of the largest countries, China, has an adoption rate of less than 3% and experiences significant reliability issues. In terms of IPv6 take-up then we can certainly see potential issues of internet fragmentation.

Internet Censorship, Blocking and Filtering

Article 19 of the *Universal Declaration of Human Rights* states that:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The notion, therefore, that access to information should be restricted, clashes with a fundamental core belief in the modern age.

Lessig's argument that code can be used to restrict access is again valid here, since, with a system built on code, information can be easily blocked or restricted based on parameters set within the code. We can see this in internet filtering systems on a daily basis, for instance within public services offering internet access such as public libraries and schools, where internet filters on local servers are often utilised to restrict access to information deemed to be inappropriate.

Decisions, then, within organisations offer us a first glance at the challenge of restricting access to information on the internet. Another concern, perhaps greater, is the desire on the part of governments to restrict access to information for an entire country. The 2015 *Freedom on the Net* report highlighted that internet freedom globally had declined for the fifth consecutive year. [14] Running a wide range of proscribed categories, topics such as satire, blasphemy, criticism of authority, comments on corruption and social commentary were all areas where countries were increasingly blocking access. [15] The report also highlighted increasing moves on behalf of governments to proactively make takedown requests for content, as opposed to blocking. While arguably less draconian, such requests are still often secret, between a government agency and host organisation of the information or data. In summary, the *Freedom on the Net* report estimates that only 31% of the global population currently reside in countries where access to the internet is completely free from government restriction. [16]

Another modern concern built on the diplomatic antipathies of the past is the development of cyber espionage and cyber warfare. While computer hacking has been around for decades, films from the 1980s such as *Wargames* pictured hackers potentially beginning nuclear wars, the reliance of modern societies on the internet and the services provided by it make cyber espionage and cyber warfare significant dangers to the autonomy of states, and to individuals. Recent high-profile incidents have seen situations such as North Korea claim responsibility for hacking into the network of the Sony Corporation. We obviously rarely hear about states hacking other states, as governments generally do not like their vulnerabilities being exposed publicly, yet the dangers of states bringing down important areas of the network infrastructure of their enemies is a real one that has the potential to do significant damage. The potential here is, of course, economic, DDoS attacks on

[14] Freedom House*, Freedom on the Net* 2015

[15] *Ibid.* p.4-5

[16] *Ibid.* p.8

companies making them unable to trade, but also social, attacking systems that support vulnerable citizens like hospital networks, or transport and transit systems.

There is an argument then for governments to advocate that protection of the interests of the state and citizens within it need to take into consideration legislation on such issues. Yet the differences in how countries deal with such issues can be stark. The Gary McKinnon case, where a hacker based in London accessed several US government networks, including NASA and the Department of Defense highlighted both jurisdictional and cultural problems. The law he was accused of breaking in the US was linked to terrorism and could command decades in prison on conviction, whereas the UK law at the time in comparison amounted to punishments that could be construed as a slap on the wrist. It is unlikely we will ever have an internationally agreed set of parameters on this issue, despite agreements like the *Convention on Cybercrime*.

Conclusions

Based on this short discussion of some of the key themes identified by Hill as being at the centre of Internet governance concerns, internet fragmentation is a reality, and the potential for it to transform the experiences of the netizen in various ways is real. Rather than standing outside of the values and norms of traditional society and values, perhaps the issue is that we may have to resign ourselves to the internet merely being another extension of ordinary society. In doing so concerns of fragmentation lessen because our expectations of it also lessen. Perhaps the ideal of a universal experience in a new information paradigm was always one that was out of reach, however, it does seem that Barlow's assertion to governments that they had "no sovereignty where we gather"[17] is one that is further away than ever.

References

Cerf V, Ryan P and Senges M, 'Internet Governance Is Our Shared Responsibility' (2014) 10 *I/S: A Journal of Law and Policy for the Information Society* 1

Freedom House. *Freedom on the Net* 2015. 2015.

French RD, 'Net Neutrality 101' (2007) 4 *University of Ottawa Law & Technology Journal* 109

Hill JF, *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers* (Belfer Center, Harvard Kennedy School 2012)

McCartney D, 'Law and the Open Internet' (2011-2012) 64 *Federal Communications Law Journal* 493

DMcM/10-2018

[17] Barlow, J.P. *A Declaration of the Independence of Cyberspace*. https://projects.eff.org/~barlow/Declaration-Final.html