Regulation and Infrastructure

1

Internet Regulation

Andres Guadamuz*

How can we regulate the Internet? This seemingly innocent question has been the subject of countless books and articles for just over the past 20 years. Part of the reason why it continues to be a vibrant and relevant topic is the difference of opinions on what is going on. On the one hand, we have those who believe that the Internet is a free and open space that requires no regulation, and/or is incapable of being regulated. On the other hand, we have those who think that regulation is not only desirable, but that the Internet as it exists now is completely regulated because of the prevalence of state surveillance, and that all semblance of freedom is a mere illusion.

I. The Internet

The Internet has become an integral part of our lives, but if you were to ask the average user about how it works, they would not be able to provide any details other than the fact that it is a medium to transmit information. This is as it should be; as technologies become widespread it is not necessary to understand how they operate—it is possible to drive a car without understanding the intricacies of the internal combustion engine.

However, when it comes to regulating the Internet, it is useful to at least have an idea of what lies under the hood, since it is difficult to try to exert some control over something that one does not understand.

From a regulatory perspective, the first element that should be remarked upon is that the Internet is a 'network of networks'[1] that operates using common protocols designed to ensure resilience, distribution, decentralisation and modularity. It is now part of the history of the Internet that started as a military programme intended to create a communication infrastructure that could survive a nuclear strike. To achieve this objective, a communication

* Some of the ideas presented in this chapter can be found in my book on complexity and Internet regulation: *Networks, Complexity and Internet Regulation: Scale-Free Law* (Cheltenham, Edward Elgar, 2011). This chapter is both an update and a reworking of some features of the book.

[1] Jianxi Gao Daqing Li Shlomo Havlin (2014) 'From a single network to a network of networks' 1:3 National Science Review 346.

network needs to be decentralised, with no central point or governing node. Similarly, communications must be able to be broken down and sent through various links in the network, only to be put together automatically by the recipient. The network will also be made of heterogeneous pieces of hardware that should be able to talk to each other using standard communication tools, and everything should have simplicity and modularity in mind.[2]

The best way to understand the Internet is to separate its architectural features in layers of functionality. By doing this, it is possible to identify the various elements with regards to the function that they serve. The Internet has four layers:

1. **Link layer.** The link layer consists of protocols that allow connection of a host with gateways and routers within a network, usually a large area network (LAN) (eg Ethernet protocols).
2. **Transport layer.** This provides end-to-end protocols for communication between hosts in the system, such as the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).
3. **Internet layer.** Because the Internet is a network of networks, every computer connected to it must be able to find its components. The Internet Protocol (IP) fulfils this function, and is differentiated from the application and transport layers by the fact that it does not consist of instructions to reach a destination, or is used to make the actual communications, but it allows data packets to reach their destinations by allowing identification of participating computers based on their IP address.
4. **Application layer.** This is the top communication level made up of protocols for user applications such as sending mail (Send Mail Transfer Protocol, or SMTP), sending files (Hyper Text Transfer Protocol, or HTTP); it also includes protocols used for system support, such as that which identifies servers in the system by name instead of IP address (Domain Name System, or DNS).

The idea behind the above classification for regulatory purposes is that some elements are so fundamental to the functioning of the Internet that they cannot be regulated. The first three layers are specifically about communication between networks and computers, and they are made up of protocols that have been established by the various standards-setting bodies such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Internet Engineering Steering Group (IESG), the Internet Architecture Board (IAB) and the Internet Society (ISOC). The role of the first layers is to distribute information across the networks.

[2] B Carpenter, 'Architectural Principles of the Internet' (Internet Architecture Board Paper, 1996), available at www.ietf.org/rfc/rfc1958.txt (last accessed 19 June 2018).

The application layer is different. Most user activity takes place here, and this is where most communication subject to regulation will take place. The standards used to get communications from one computer to the other tend to be irrelevant for regulators, other than perhaps being of interest from a governance perspective. However, it is the actual communications that matter, and these will take place through applications.

Having said that, the communication layers may be relevant for the type of regulation that is proposed. For example, a country that wants to control the flow of data coming in and out of its jurisdiction would place technical controls at the Internet layer level in order to filter or block content before it reaches its destination.

II. A Tale of Two Internets

Perhaps the best way to explain the two opposing views of Internet regulation is by contrasting two very distinct case studies that exemplify the difference in experience and perception that lead us to see the Internet in such a different light.

A. The Dark Web

As it was explained above, the Internet is made up of common protocols that allow users to communicate and exchange information with one another. The 'visible' Internet makes use of the four layers, and it consists of shared applications such as the World Wide Web, email, social media apps, games, file transfers, etc. Users connect to the network using the communication layers, and they can connect to one another using the application layer.

Beneath the visible Internet exists a network that not many know how to access, known as the Dark Web (or Dark Net). It uses the Internet's own transport layers, but it consists of applications that are shared by a few technically-minded users. This facilitates a space that is rarely visited, highly encrypted and seldom regulated.

James Bartlett describes the Dark Web as follows:

> For some, the dark net is the encrypted world of Tor Hidden Services, where users cannot be traced and cannot be identified. […] It has also become a catch-all term for the myriad of shocking, disturbing and controversial corners of the Net – the realm of imagined criminals and predators of all shapes and sizes.[3]

[3] J Bartlett, *The Dark Net: Inside the Digital Underworld* (London, William Heinemann, 2014).

One of the most visible Internet applications is the World Wide Web, and we commonly surf through it with web browsers that can read web pages created using the Hypertext Markup Language (HTML). However, because the Internet is decentralised and modular, it is possible for anyone to come up with new applications and protocols that use the communication layers. I could program a new browser that uses my own application protocol, and as long as there is someone else using it, then that would still be part of the Internet, but it would be invisible for most users.

One such application is the Tor Browser, which uses the TOR Hidden Service Protocol to connect computers that are also connected to the Internet.[4] This is a communications protocol created by a group of encryption enthusiasts designed to anonymise data transferred through the Internet by using voluntary relays and routers that mask a user's identity to prevent traffic snooping and surveillance. By installing the Tor Browser on their computers, users can view websites that are not accessible through a mainstream browser like Firefox or Chrome.

The anonymous nature of the Dark Web makes it possible to post any type of content, and using anonymous and decentralised payment methods like Bitcoin, users can purchase almost anything they desire.[5] At the time of writing, it was possible to access pages on the Dark Web advertising various drugs, UK passports, US identification documents, hacking services, stolen credit cards and hacked social media accounts.

All of this has led the Dark Web to gain a difficult reputation, coupled by the publicity gained in the trial of Ross Ulbricht, the operator of the Silk Road website, a deep web marketplace for any sort of illegal material.[6]

The presence of such vast and unregulated space tends to lend credence to the idea that the Internet cannot be regulated.

---

[4] D Dingledine et al, 'Tor: The Second-Generation Onion Router' (2004), available at https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf (last accessed 19 June 2018).

[5] For more about Bitcoin, see A Guadamuz and C Marsden, 'Blockchains and Bitcoin: regulatory responses to cryptocurrencies', (2015) 20(11) *First Monday*, http://dx.doi.org/10.5210/fm.v20i12 (last accessed 21 June 2018).

[6] J Mullin, 'Ulbricht Guilty in Silk Road Online Drug-Trafficking Trial' *Ars Technica* (4 February 2015), available at https://arstechnica.com/tech-policy/2015/02/ulbricht-guilty-in-silk-road-online-drug-trafficking-trial/ (last accessed 19 June 2018).

B. Snowden's Internet

Thanks to the series of revelations made by former National Security Agency (NSA) contractor Edward Snowden,[7] we have a troubling picture of extreme control due to mass surveillance conducted by the NSA in the US, and the Government Communications Headquarters (GCHQ) in the UK.

Although the Internet is supposed to be a decentralised, distributed and open telecommunications network, the surveillance revelations have unearthed a much more controlled and centralised system than previously thought possible. Snowden left his life as a contractor and travelled to Hong Kong where he contacted journalist Glenn Greenwald and filmmaker Laura Poitras to whom he gave access to a series of files that laid bare the extent of state surveillance.

The revelations showed a troubling amount of surveillance at all levels, and it is not this chapter's remit to cover these in detail. Following the above classification of the Internet's architecture into layers, it is possible to highlight just some of the issues uncovered:

1. **Link layer**. The Tailored Access Operations (TAO) is the NSA's powerful hacking unit, which specialises in breaking into a target's every communication by tinkering with their access points to the network.[8] The unit uses built-in backdoors in hardware such as routers to tap into people's connection at the point of origin.
2. **Transport layer.** The NSA has managed to tap some of the most important underwater cable systems, which make up the very backbone of the Internet.[9] The tapping is possible because the communications in the transport layer are not encrypted by default.
3. **Internet layer.** This is related to the above paragraph. It has been revealed that the NSA may have had a hand in the lack of default encryption in the Internet layer protocols (TCP/IP), as Vint Cerf, one of the fathers of the Internet, has claimed that he was stopped by the NSA from including an encrypted protocol into the transport layer.[10]
4. **Application layer.** One of the most troubling revelations has been that the NSA has managed to obtain collaboration from technology firms to conduct surveillance within applications, including allegedly secure and encrypted communications like Skype.[11]

---

[7] L Harding, *The Snowden Files* (London, Guardian Faber, 2014).
[8] J Applebaum et al, 'Inside TAO: Documents Reveal Top NSA Hacking Unit' *Der Spiegel* (29 December 2013), available at www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html (last accessed 19 June 2018).
[9] *Ibid*.
[10] P Roberts, 'CERF: Classified NSA Work Mucked Up Security For Early TCP/IP' *Veracode* (3 April 2014), available at www.veracode.com/blog/2014/04/cerf-classified-nsa-work-mucked-up-security-for-early-tcpip (last accessed 19 June 2018).
[11] J Ball et al, 'Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security' *The Guardian* (6 September 2013), available at www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (last accessed 19 June 2018).

> The project Sigint, which stands for signals intelligence, creates partnerships with developers and companies to build exploits into telecommunication tools.

All of the above speaks of a much more controlled Internet, filled with taps, exploits and collusion on the part of industry, culminating in an unprecedented level of surveillance.

C. Will the Real Internet Please Stand Up?

If one reads each of the above two sections separately, then one would conclude very different things about the nature of the Internet, and the need for regulation.

If one were to read only stories about the Dark Web, one would be likely to conclude that the Internet is a lawless anarchic space filled with pornography, drugs and illegal weapons, where paedophiles and terrorists have a free pass.

If one reads about the Snowden revelations, then one could conclude that we live in a dictatorial dystopia of Orwellian proportions, where shadowy agencies monitor our every thought.

As is often the case, the truth lies somewhere in the middle.

The Internet presents a space that is difficult to regulate despite the existence of the surveillance apparatus described above. While it is relatively easy for most people to be identified when they do something online, there is still some level of anonymity in the network, and there is growing evidence that any attempt at exercising enforcement online will result in increased levels of purposeful and directed anonymisation. For example, a study in Sweden found that when regulators tried to enforce new legislation to curb file-sharing, the number of users of anonymous services such as proxies and virtual private networks rose.[12] Similarly, jurisdiction continues to be an issue, evidenced by the fact that criminal operations move online because enforcement tends to be ineffective,[13] and the costs attributed to cybercrime continue to rise.[14]

---

[12] S Larsson and M Svensson, 'Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorised File-sharing' (2010) 2(4) *Policy & Internet* 77.
[13] J Naughton, 'These Days Crime Doesn't Pay… Unless it's Done Online' *The Guardian* (29 March 2015), available at www.theguardian.com/commentisfree/2015/mar/29/cybercrime-online-government-cuts-crime-statistics (last accessed 19 June 2018).
[14] R Anderson et al, 'Measuring the Cost of Cybercrime' *Workshop on the Economics of Information Security* (Stockholm, Sweden, 2012), available at www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf (last accessed 19 June 2018).

On the other hand, despite the large surveillance apparatus laid bare by Snowden, this has not yet been translated into more control of everyday Internet transactions. Users continue to share files infringing copyright, and in general people manage to use the network in ways that would be expected even without surveillance. But what is emerging is a more centralised experience for large numbers of users, both at the private and public level.

First, state control is possible – the Chinese Internet, with its built-in filtering and censorship mechanisms, demonstrates a more controlled experience for the largest Internet demographic in the world. Closer to home, court injunctions[15] have successfully blocked access to hundreds of infringing sites, such as The Pirate Bay and Isohunt, and while such blocking is easily circumvented by experienced users, for the large majority the filtering and blocking successfully restricts access to illegal material.[16]

Second, the everyday experience of millions of users is predicated on what private enterprises show them. As more and more people browse through mobile applications, their online experience is defined by the app developer. The level of control that these private enterprises hold can be evidenced by the fact that for a growing number of users, the Internet doesn't even exist; for example, in several countries in Asia the number of self-identified Facebook users is larger than the number of Internet users, which leads researchers to believe that in many territories people mistake Facebook for the Internet.[17]

Thus a more nuanced picture of the Internet begins to emerge. A minority of technically-oriented users operate in heavily encrypted spaces with near-impunity from regulation, while a large number of people suffer constant regulation through censorship, blocking and filtering of content. A person's experience of the Internet will therefore be heavily dependent on education, resources and geographical location.

In other words, the Internet resembles more and more the inequality of 'real' life, but where the one per cent has been replaced with a techno elite minority.

III. Regulation Theories

[15] A series of blocking orders that start with *Twentieth Century Fox Film Corporation & Anor v Newzbin Ltd* [2010] EWHC 608.
[16] eg, this study suggests dropping torrent usage due to the increase in legal streaming use: Sandvine, *Global Internet Phenomena Report* (2013), available at www.sandvine.com/downloads/general/global-internet-phenomena/2013/2h-2013-global-internet-phenomena-report.pdf (last accessed 19 June 2018).
[17] L Mirani, 'Millions of Facebook Users Have No Idea They're Using the Internet' *Quartz* (9 February 2015), available at https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/ (last accessed 19 June 2018).

A. Plus ça change?

It is a common display of modern hubris to believe that the Internet is new in a fundamental way. We see the world around us and notice the impact in almost everything that we do, from planning a trip to driving to work. The advent of the Internet was met with some grandiose statements about how it would herald a new golden era of prosperity and global understanding, an age of 'computer-aided peace'.[18] In 1997, Nicolas Negroponte predicted that in 20 years' time children 'are not going to know what nationalism is'.[19] However, 20 years on, such statements look laughable.

The problem is not only a certain lack of imagination on the part of technology enthusiasts, but also a lack of historical awareness. Undoubtedly there are many important developments both in regulation and communication that have been experienced before, and it is pertinent to remember that many of the debates that we tend to think of as inherently digital were experienced before during the adoption of different technologies.

One of the best examples of this is encapsulated in Standage's seminal book *The Victorian Internet*,[20] which draws many parallels between the rise of telegraphy as a means of communication in the nineteenth century, and the rise of the Internet. These parallels include the misuse of the technology for fraudulent purposes, the creation of a highly-skilled technical class of users and operators and the social changes that it brought.

Our current obsession with technology is often similar to earlier debates about the role of communication and media in society. In a now famous *Newsweek* cover in 1970, the magazine asked whether privacy was dead, with a cartoon depicting an anxious couple harassed by computers, telephones, cameras and microphones.[21] One could easily update that cover with modern concerns such as smartphones, CCTV and drones.

As early as 1983, Ithiel de Sola Pool was already discussing some of the social changes and the societal implications of electronic communication before the digital era, identifying key elements about media ownership, distance, centralisation, and privacy. In his book *Technologies of Freedom*, he wrote:

---

[18] M Dertouzos, *What Will Be: How the World of Information Will Change* (New York, Harper Collins, 1997).
[19] 'Negroponte: Internet is Way to World Peace' *CNN* (25 November 1997), available at http://edition.cnn.com/TECH/9711/25/internet.peace.reut/ (last accessed 19 June 2018).

[20] T Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's on-Line Pioneers* (San Francisco, Berkley Books, 1999).

[21] The cover can be found at https://www.thedailybeast.com/is-privacy-dead (accessed 21 June 2018).

> The exercise of regulation and control over communication is a central concern in any treatise of freedom. How much control are policy makers allowed to exercise? What are the limitations on them […]? May they censor? May the license those who seek to communicate? What norms control the things that communicators may say to each other? What is libel, what is slander, what violates privacy or security? Who is chose to enforce these rules and how?[22]

These questions are just as relevant today; one could easily ask them of the phenomenon of social media. It is logical that we should consider similar questions concerning the regulation of technology, because the very act of regulation hinges on the issues of power and control, and these do not tend to change with different technologies. What changes are the players, and to a large extent the subject of regulation.

Braman makes an excellent point when talking about the changing regulatory landscape as seen by those who are subject to regulation.[23] She comments that in the pre-digital era, media regulation used to be directed almost exclusively at professional entities and organisations. With the Internet, we are witnessing a democratisation of the application of media policy and regulation in fields such as defamation and copyright. Therefore, Internet regulation has shifted from concerns about direct regulation and has moved towards discussion about intermediary liability.[24]

So, while many of the themes of Internet regulation may remain the same over the years, we can begin to identify unique features that make the Internet subject to different rules, raising the question of whether it is possible to regulate it at all.

B. The Return of Cyber-Libertarianism

The idea of the Internet as a separate space subject to different laws and regulations is as old as the term Cyberspace. In some of the most influential science fiction depictions of virtual realities in novels like *Neuromancer*,[25] *Snow Crash*,[26] and *Ready Player One*,[27] the Internet tends to be depicted as an almost different physical reality that is subject to its own rules.

---

[22] I de Sola Pool, *Technologies of Freedom* (Cambridge, Massachusetts, Harvard University Press, 1983) 9.

[23] S Braman, 'Where has Media Policy Gone? Defining the Field in the Twenty-First Century' (2004) 9(2) *Communication Law and Policy* 153.

[24] See, eg, D Mac Sithigh, 'The Fragmentation of Intermediary Liability in the UK' (2013) 8(7) *Journal of Intellectual Property Law & Practice* 521.

[25] W Gibson, *Neuromancer* (London, Harper Collins, 2011).

[26] N Stephenson, *Snow Crash* (London, Penguin, 1994).

[27] E Cline, *Ready Player One* (London, Arrow, 2012).

The early Web did feel a bit like an unregulated frontier, particularly because regulators were slow to respond and were very much taken aback by the potential of the new technology and the appearance of a global communications network that seemed to be immune from regulation. In an often-cited work on the topic, lyricist John Perry Barlow wrote his *Declaration of Independence of Cyberspace*, in which he set out to attack government intervention in Cyberspace, favouring a quasi-libertarian self-regulated approach. He wrote:

> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live. [...] Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge.[28]

Barlow believed that Internet communities would be able to exercise self-regulatory control because governments would not be able to intervene.

Other commentators and scholars adopted Barlow's ideas in the late 1990s, believing that it would be difficult to subject the Web to traditional regulatory methods. The understanding at the time was that the Internet could not be controlled in any effective manner, and so several models of self-regulation were proposed that were intended to organise the network in some coherent fashion.[29] Of note amongst these theories is Post and Johnson's Net Federalism.[30] They argued that Cyberspace is a separate entity clearly bordered with the physical world, and consequently it should be treated as an independent regulatory sphere for all legal purposes. Because the Internet would still require some form of regulation, they argued that the Web should be able to assemble its own legal institutions in a manner similar to the creation of federal states brought together under a unifying ideal. These self-regulated federal 'states' would generate their own sets of rules consistent with practice in that part of Cyberspace.[31]

While some of the arguments in favour of cyber-libertarianism might be persuasive, Barlow, Post and Johnson completely underestimated the regulatory push from governments

---

[28] JP Barlow, *A Declaration of the Independence of Cyberspace* (Electronic Frontier Foundation, 1996), available at www.eff.org/cyberspace-independence (last accessed 19 June 2018).
[29] A comprehensive review of most of these ideas can be found in G Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21(2) *University of New South Wales Law Journal* 593, available at www.austlii.edu.au/au/journals/UNSWLJ/1998/52.html (last accessed 19 June 2018).
[30] DR Johnson and DG Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367.
[31] Other works of note are J Reidenberg, '*Lex Informatica*: The Formulation of Information Policy Rules through Technology' (1998) 76 *Texas Law Review* 553; and J Boyle, *Shamans, Software, and Spleens: Law and the Construction of the Information Society* (Cambridge, Massachusetts, Harvard University Press, 1996).

and international organisations that would take place.[32] Even back in the late 1990s, several authors criticised the cyber-libertarian ideas of unregulated spaces. In particular, Boyle[33] seems to have understood that the premise behind the theories of the impossibility of exercising any credible governance over Cyberspace was not only wrong-headed, but rested on completely untested hypotheses. In his view, cyber-libertarianism was blind to the many avenues of control available to public regulators.

Nonetheless, cyber-libertarianism continues to endure even to this day. Part of its baffling resilience might arise from the sense of regulatory despair that is often awakened when new technological changes take place. It is interesting how the 'Internet cannot be regulated' mantra is resurrected every few years when we are presented with a new advance online. This was true of virtual worlds, peer-to-peer (P2P) file-sharing, 3D printing, social networks, cryptocurrencies and wearable technology, to name just a few examples.[34] When presented with challenges, many tend to revert to a cyber-libertarian default, declaring the new technology as impossible to regulate. This enduring feature of cyber-libertarianism may be fuelled by nothing more than unfamiliarity with either the new technologies or the history of the Web. As the Internet matures, it seems like every new generation believes that its online experience is unique to the one that came before it.

But the real reason for the return of cyber-libertarianism may be more normative than descriptive. With Snowden's revelations, we are being presented with a dystopian surveillance apparatus that does not resemble the free and open Internet ideal that was originally envisaged. On this view, it is not so much that the Internet *cannot* be regulated, but that it *should not* be regulated. Snowden has given us the perfect excuse, if any was needed, to further distrust regulatory structures. During the closing statements at the 2014 Internet Governance Forum (IGF) in Istanbul, Milton Mueller proposed that Barlow was worth a second look, and postulated the idea of an Internet Nation:

> Barlow's idea that the internet was immune from control by existing governments has been discredited. But remember, Barlow drafted a declaration of independence. Such a declaration does not necessarily mean that existing nations have no power; it means that the residents of cyberspace want a distinct nation of their own. […] There is nothing terribly crazy or controversial about the concept of an Internet community. Clearly, the Internet provides the basis for a community with its own interests, an incipient identity, its own norms and modes of

[32] eg, the World Intellectual Property Organisation (WIPO) Copyright Treaties. See J Sheinblatt, 'The WIPO Copyright Treaty' (1998) 13 *Berkeley Technology Law Journal* 535.
[33] J Boyle, 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors' (1997) 66 *University of Cincinnati Law Review* 177.
[34] See, eg, A Guadamuz, 'Back to the Future: Regulation of Virtual Worlds' (2007) 4(3) *SCRIPTed* 242.

> living together. And it is only a small step from community to nation. A nation is just a community that wants its own state.[35]

This is perhaps a proposition that requires a second look. Many of those who laughed at the idea of cyber-libertarianism did so from the perspective that it clashed with practice, and that governments seemed quite adept at regulating certain aspects of the online experience. But perhaps we were asking the wrong question, and we should now be asking whether such regulation is desired.

C. Regulating the Gateways

While cyber-libertarianism may be experiencing a comeback, it still needs to confront the cold reality of power struggles. The rise of Napster in 1999 and the later emergence of P2P file-sharing networks,[36] served as clear reminders of the difficulties of enforcing the law in the digital domain. The near-limitless availability of illicit materials online coupled with the widespread availability of infringing content gave the impression that the Internet was a medium where no regulation was possible. Nonetheless, despite the glaring failure in shutting down file-sharing networks, the early years of the twenty-first century witnessed the deployment of relatively successful regulatory approaches by many national governments.

The landscape of Internet regulation up until around 2000 was a mixture of cyber-libertarianism and half-hearted legislative solutions. The Internet was a global, distributed and borderless network because it had been designed as such. It also demonstrated resilience because of its origins as a military network whereby its design meant that communications could easily route around damage to any one node in the network. Castells describes this as 'architecture of openness'.[37] Vint Cerf, one of the fathers of the modern Web, went as far as stating that the Internet traffic was 'totally unbound with respect to geography'.[38]

However, as Goldsmith and Wu rightly point out, this initial architecture was not entirely set in stone, and unsurprisingly, it soon became clear that national governments were

[35] M Mueller, 'Internet Nation?' (Internet Governance Project, 5 September 2014), available at www.internetgovernance.org/2014/09/05/internet-nation/ (last accessed 19 June 2018).
[36] See S Smith, 'From Napster to Kazaa: The Battle over Peer-to-Peer Filesharing Goes International' (2003) *Duke Law & Technology Review* 8.
[37] M Castells, *The Internet Galaxy: Reflections on Internet, Business, and Society* (Oxford, Oxford University Press, 2001) 26.
[38] As cited by L Guernsey, 'Welcome to the Web. Passport, Please?' *New York Times* (15 March 2001), available at www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html (last accessed 19 June 2018).

attempting to draw borders in Cyberspace.[39] The most successful attempt to do so was the segregation of the Internet into national intranets. While the Internet was supposed to be globally distributed, several countries started redesigning the entry points into their national networks in order to impose screening mechanisms that would allow them to filter out undesired content.

This state of affairs is a logical result of the manner in which the Internet grew. While the global architecture of the Internet as a distributed network still holds true because of the existence of routers and distributed protocols, the actual physical Internet is often centralised. In the early days of the Internet, a lot of information was spread through the telephone network, which ensured a high, albeit expensive, distribution ratio.[40] Later, a high-speed backbone had to be built to accommodate larger amounts of information being spread throughout the system, first copper cables and satellites, and later optical cables.[41] The end result was a more centralised Internet than was originally envisaged, as the router distribution worked within connected nodes. This can be explained using the UK as an example: the country has many roads, but not being connected to continental Europe, it relies on ports and airports as communication hubs. The modern Internet looks something like that, with physical connections akin to ports where most of the information comes through, and then it is distributed using routers and hosts in the manner in which it was intended. Many countries have reduced the number of physical entry points to their internal networks, effectively creating Internet chokepoints. If a government controls these gateways, then it will be easier to exercise control over the Internet in that particular country as a whole.

Unfortunately, there are a growing number of examples of just how effective such chokepoint regulation may be. By far the best example of this is the so-called Great Firewall of China, known there as the Golden Shield Project. The Great Firewall is a multi-layered technological solution that takes advantage of the fact that the Chinese Government controls the few Internet gateways into the larger Chinese Internet. This allows the Government to impose effective filtering restrictions to incoming Internet traffic by various means. The most crucial is the filtering of IP addresses originating from blacklisted services, which range from

[39] JL Goldsmith and T Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford, Oxford University Press, 2006) 58.
[40] Some early networks, such as Fidonet, even sent all of their packets during cheap-rate calling times, see J Naughton, *A Brief History of the Future: The Origins of the Internet* (London, Phoenix, 2000) 190.
[41] B Leiner et al, *A Brief History of the Internet* (Internet Society Paper, 2000), available at www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf (last accessed 19 June 2018).

Blogger to Sex.com.[42] While this is in no way a perfect system, it does allow the Chinese Government a level of influence that was thought impossible with the distributed architecture. The Great Firewall works by deploying hardware routers at each of the entry points into the country. These routers are given lists of banned IP addresses, so when an Internet host within China makes a request to access a banned site, the router does not forward the request to the target host, so the site appears not to exist, and a network error message is returned to the client.[43]

Another well-documented phenomenon was the disconnection of the Egyptian Internet during the Arab Spring. On 27 January 2011 at around 10.30 GMT, the entire Egyptian Internet was disconnected from the rest of the world by Egyptian authorities to respond to widespread protests that were made using social media to communicate and organise.[44] This was possible because Egypt, like many other countries in the Middle East, has a national firewall consisting of an extra layer of Internet servers that mediate all traffic in and out of the country through servers running the appropriately named Border Gateway Protocol (BGP). Egyptian authorities managed simultaneously to shut down 3,500 BGP routes into the country, which meant that more than 90 per cent of all traffic in and out of the country could not get through.[45]

Therefore, it has become clear then that the most effective regulatory solution to online content is to exercise control at the access points. This regulation model has been replicated in many other countries,[46] proving that the Internet is decreasingly distributed, and looks increasingly like a network of self-enclosed city states with connecting ports.

Moreover, private enterprises have been co-opted as regulators of their own environments, in what Laidlaw describes as gatekeepers.[47] She identifies two types of gatekeepers—those who broadly control the flow of information, and what she calls Internet information gatekeepers, who 'as a result of the control impact participation and deliberation

[42] Goldsmith and Wu (n 38) 92.
[43] Goldsmith and Wu (n 38) 92–94.
[44] C Williams, 'How Egypt Shut Down the Internet' *The Telegraph* (28 January 2011), available at www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html (last accessed 19 June 2018).
[45] L Greenemeier, 'How Was Egypt's Internet Access Shut Off?' *Scientific American* (28 January 2011), available at www.scientificamerican.com/article/egypt-internet-mubarak/ (last accessed 19 June 2018).
[46] For a comprehensive survey, see J Zittrain et al, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, Massachusetts, MIT Press, 2007).
[47] E Laidlaw, 'A framework for identifying Internet information gatekeepers' (2010) 24(3) *International Review of Law, Computers & Technology* 263.

in the democratic culture'.[48] Under this framework, large parts of the online environment become regulated by private entities through end-user licence agreements and terms of use, where the gatekeeper can unilaterally remove content with little recourse to the creator. The role of intermediaries as gatekeepers becomes an integral part of the regulatory arsenal, and makes it difficult to sustain the contention that the Internet is an environment devoid of any control.

It must be pointed out that the regulation at the gateway level has interesting side effects for regulatory purposes. The first interesting characteristic is a less decentralised and highly balkanised system where countries exercise internal control. The second is that private enterprises exercise an increasingly powerful level of control over their users, either at the prompting of government, or on behalf of other private actors. The result is a much more centralised environment that does not conform to cyber-libertarian ideals.

D. Code

Since its publication in 1999, Lessig's *Code and Other Laws of Cyberspace*[49] has become one of the more influential books on Internet regulation. In it he postulates that there are four main modes of regulation, namely markets, norms, law and architecture.[50] Most theories of regulation up until then accounted for the first three. Lessig's breakthrough came in the way in which he identified the prevalence of architectural regulation in technological settings. Lessig argued that the Internet itself is highly dependent on the technological architecture that sustains it, the 'code' in which it is written, the connectivity layers between domains, the protocols used in order to distribute information from one computer to another, the functional layers of said protocols, the domain name server system that tells one computer's location in the system, and so on.[51] Whether the Internet can be subject to regulatory control will depend entirely on its underlying architecture. For example, some of the constituent code of the Internet is open, that is, it can be inspected, copied and modified by all sorts of people. This code cannot easily be subject to government regulation. However, the protocols and communication tools that make up the online world are more critical than the underlying code because they are needed for connectivity to take place. Whoever controls the underlying 'plumbing', and the protocols, thus controls the Internet.

[48] *Ibid* 266.
[49] L Lessig, *Code: And Other Laws of Cyberspace* (New York, Basic Books, 1999).
[50] *Ibid* 88.
[51] *Ibid* 100–102.

But who writes the code? Lessig's architectural regulation suggests the existence of some form of self-ordering mechanism. He identifies the 'invisible hand' of cyberspace that exerts an ordering force into the architecture of the Internet:

> Control. Not necessarily control by government, and not necessarily control to some evil, fascist end. But the argument of this book is 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.[52]

Nonetheless, Lessig's version of the invisible hand of cyberspace is limited in that he believes that it is shaped by code. So, programmers, regulators and policymakers can make conscious decisions that shape what the underlying architecture will look like, hence exercising real control over the shape of the Web.[53] This version of self-organisation is, as a result, limited by conscious decisions, and while Cyberspace may reach its own efficient regulation, it can be subject to change.

While the original text has been updated,[54] and some of the examples feel dated, the work is still as relevant today as it was back then. As the years pass, and more technology developments arise and evolve, it becomes more evident that architectural decisions made at the outset of the development of a technology have huge implications about how it is going to be regulated.

A great example of an architectural decision that has had huge implications is one of the building blocks of the Internet, the TCP/IP protocol suite. The suite is designed to allow packets of information to reach the intended recipient, but it has a well-documented flaw,[55] namely a lack of authentication. This allows a range of common attacks, such as so-called 'IP spoofing', whereby a malicious user pretends to be sending data from an IP address other than its own. Because there is little authentication, the network assumes that it is coming from that address.[56] This security fault has also made mass surveillance easier, prompting accusations that such an oversight was a purposeful decision in order to make such control possible. Vint

[52] *Ibid* 7.
[53] *Ibid* 106–108.
[54] L Lessig, *Code Version 2.0*, 2nd edn (London, Basic Books, 2006).
[55] Identified as early as the 1980s, see SM Bellovin, 'Security Problems in the TCP/IP Protocol Suite' (1989) 19(2) *Computer Communication Review* 32.
[56] C Chambers, J Dolske and J Iyer, *TCP/IP Security* (Linux Security Document, 2001), available at www.linuxsecurity.com/resource_files/documentation/tcpip-security.html (last accessed 19 June 2018).

Cerf has even admitted that there were proposals to create a network encryption layer, but that it would require the use of encryption technology which at the time was restricted.[57]

The TCP/IP authentication vulnerability is a great example of the strengths and weaknesses of the code regulation model. At its heart, the code model relies on the informed decision of coders and policymakers, and we are expected to believe that they will make the best decisions. But this is not always the case. It is possible for regulators to build bad code into the system, and developers are humans and make mistakes as well. We may also code into place solutions that do not work, or are misguided. Brown and Marsden make this point in their book *Regulating Code*. They write:

> Regulation by code can increase the efficacy of regulation but should not be seen as a panacea. Copyright holders' hopes that 'the answer to the machine is in the machine' led them to waste almost twenty years attempting to enforce scarcity-based business models rather than innovate toward the 'celestial jukebox' that is finally emerging in products such as Spotify. Code is fundamentally a non-state-designed response that can lead to more effective solutions but will tend to undervalue the public interest and lack democratic legitimacy.[58]

Thus, code can be an empowering regulatory tool, but it can also often be misused, wittingly or otherwise. There is no such thing as an invisible hand of Cyberspace, but we are presented with a model in which programmers, regulators and policymakers make conscious decisions that shape the underlying architecture of the Internet. These decisions are in turn limited by existing technology, but also by other constraints such as the basic online structures.

It would be possible to think of code more as a regulation hierarchy, akin to the Kelsen's pyramid with constitutional norms at the top.[59] At the top of the Internet code pyramid are the foundational protocols, such as the TCP/IP suite, which gives us a clear case of a conscious architectural decision. All other Internet protocols tend to rest on the foundational ones, and therefore must respond to the existing characteristics of the network. Developers can make decisions, but those have to respond to the existing constraints.

IV. Complexity and Self-Organisation

[57] J Leyden, 'Vint Cerf Wanted to Make Internet Secure from the Start, but Secrecy Prevented it" *The Register* (7 April 2014), available at www.theregister.co.uk/2014/04/07/internet_inception_security_vint_cerf_google_hangout/ (last accessed 19 June 2018).

[58] I Brown and C Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (Cambridge, Massachusetts, MIT Press, 2013) 170.

[59] H Kelsen, *Pure Theory of Law*, 2nd edn (Clark, New Jersey, The Lawbook Exchange, 2005).

All of the above theories explain different parts of the problem of online regulation. The resistance of various corners of the Internet to regulation can explain the baffling endurance of cyber-libertarianism. It is also evident that the regulation of gateways and chokepoints has had an effect in exercising some form of control over the network. Code can help to explain how some behaviour is built into the system's architecture.

It has been the contention of the author in several works that the Internet is a complex network that displays self-organising characteristics.[60] Assuming that the Internet is a complex adaptive system subject to self-organisation,[61] one might postulate that any attempt to regulate specific elements within the network will have to take into account this important emergent attribute of the global communication system. Moreover, it may not be possible to regulate adequately online environments that display self-organising characteristics without some knowledge of the empirical and theoretical features of such environments.

The network is made up of nodes and links that grow according to power laws.[62] Older links in the network accumulate more links, and those successful nodes in turn tend to accumulate more links themselves, creating a 'the rich get richer' situation. The resulting hubs serve as important connectors within the network, which in turn explains the seemingly ordered nature of the system. The nodes themselves often cluster into small world networks where the intervening pathways between nodes tend to be short. The network is fractal in nature, meaning it has the same architectural features be it on a large or short scale, hence the suggestion that it is scale-free.

The scale-free nature of the network makes the Internet resilient to random attacks. However, this also means that other undesired networks which exist within cyberspace are also robust, such as P2P file-sharing networks, ransomware, or cybercrime rings. Similarly, because of architectural decisions made early on, the network displays high levels of centrality at the national scale.

All of these features, amongst others, offer strong evidence that self-organising forces operate online. Any regulatory effort that ignores this fact is faced with severe difficulties, as

[60] See A Guadamuz, *Networks, Complexity and Internet Regulation* (n *).
[61] Understood as a system that is capable of organising itself, see SA Kauffman, *At Home in the Universe: The Search for Laws of Self-Organization and Complexity* (Oxford, Oxford University Press, 1995).
[62] A power law is a mathematical expression that happens 'when the probability of measuring a particular value of some quantity varies inversely as a power of that value'. See MEJ Newman, 'Power Laws, Pareto Distributions and Zipf's Law' (2005) 46(5) *Contemporary Physics* 323, 323.

the same self-organising forces that shape the Internet's architecture are also working to undermine and even defeat regulatory action.

The father of self-organisation studies in social systems is Niklas Luhmann, particularly his influential theory of autopoiesis.[63] In its broadest sense, Luhmann's theory of autopoiesis matches what we have witnessed online, as he defines it as social systems that respond to internal stimuli instead of relying on external elements; these elements come together to generate stability in the system. It is a common misunderstanding that self-organisation causes chaos,[64] when in reality most chaotic systems tend towards stability in the long run, much in line with what are known as 'fitness landscapes'.[65] If we think of the Internet as an autopoietic system, then we should conclude that it becomes organised because the interaction of its parts favours clustering and stability in order to manage complexity.

When presented with autopoietic systems, regulation theories have two possible strategies. One could accept that the network responds to its own self-organising elements, and therefore cannot be governed. If this is the case, then regulation is not possible. The postulated theory of self-organisation of the Internet adopts the opposite view, that self-regulation need not mean that governance of the system is impossible. While this may be optimistic, it is the only viable avenue to take if one wishes to undertake regulatory efforts. To fail to do this would be to fall prey to an anarchic and/or cyber-libertarian view of governance, where everything is left to the self-organising powers of the system. Even in the face of contradictory evidence, I adopt an optimistic view of regulation, and will assume that some form of order outside of the regulatory effort is possible.

Within the optimistic regulatory philosophy, we could try to build the system to fit the regulatory goals. Following the idea presented in Lessig's *Code*,[66] regulation strategies can be built into the system, assuming that this will seed the elements around which self-organisation will occur. As stated, complex systems will usually order themselves at fitness peaks of higher order. If we know how self-organisation works within the network, then we can try to code situations that will constitute fitness peaks in the overall landscape.

---

[63] Literally meaning self-creation. See N Luhmann, *Social Systems* (Stanford, Stanford University Press, 1995) 22.
[64] Chaos in the strict mathematical sense, meaning that rendering long-term prediction is impossible in general. See KT Alligood, *Chaos: An Introduction to Dynamical Systems* (New York, Springer-Verlag, 1997).
[65] SA Kauffman and EW Weinberger, 'The NK Model of Rugged Fitness Landscapes and its Application to Maturation of the Immune Response" (1989) 141(2) *Journal of Theoretical Biology* 211.
[66] Lessig (n 53).

There are two examples that serve to illustrate opportunities for engineered self-organisation. First, in the fight against P2P file-sharing, it seems evident that the networks are robust self-organising entities. But what would happen if one built a network architecture that specifically targets such networks? While there have been some attempts to attack the networks in this manner, perhaps more strict legislation that tackles not the infringers, but the architecture, would have more chance of success. Second, some forms of cybercrime rely heavily on the current open and centralised Internet architecture. A more tightly regulated network, with more gateways and intermediaries, may sacrifice the Web's dynamic nature, but may also seriously hinder some forms of cybercrime, particularly denial of service attacks, spam and phishing.

The optimistic view of regulation also presents opportunities for smarter regulatory efforts by informing decision-makers and stakeholders about the way in which the target system operates. Any attempt to legislate in the areas covered by Internet regulation, such as privacy, copyright and cybercrime, must consider the emergent traits of Cyberspace. At some point policymakers will realise that their regulatory efforts are having no effect, and hopefully they will look at some of the research highlighted in this work in search of evidence.

To recap, the self-organisation theory of Internet regulation is as follows: the Internet is a complex system that displays self-organisation. In order to efficiently and successfully regulate the digital environment, it is imperative that one understands how it is organised, what characteristics are present, what elements act as fitness peaks and how architectural decisions affect its emergent features.

V. Epilogue: The Centrality Menace

On 2 March 2013, an unprecedented (and under-reported) event in the history of the Internet took place. A small technical fault arising from a software update took out 785,000 websites that use the popular content delivery network CloudFlare for over an hour.[67] While some downtime is to be expected, what is remarkable about this incident is that it should never have happened. The Internet is planned with a very clear idea in mind, and that is resilience. It was designed in part to respond to an all-out nuclear strike on the communications infrastructure

[67] R Dillet, 'CloudFlare Was Down Due To Edge Routers Crashing, Taking Down 785,000 Websites Including 4chan, Wikileaks, Metallica.com' *TechCrunch* (3 March 2013), available at https://techcrunch.com/2013/03/03/cloudflare-is-down-due-to-dns-outage-taking-down-785000-websites-including-4chan-wikileaks-metallica-com/ (last accessed 19 June 2018).

of the US, and therefore it had a clear design goal that has decentralisation at its core. The idea is that all traffic is distributed through other nodes in the network, so if any individual node is knocked down, then traffic should be able to be re-directed through another pathway. The CloudFlare outage was possible because the modern Internet is starting to ignore and bypass this very basic rule for convenience purposes. We are increasingly seeing more centralisation as part of the network, and this spells trouble not just from a technical standpoint, but also with respect to how we are sleepwalking into a more centralised, more regulated, and less open global network.

Anyone who is aware of the decentralised nature of the Internet will undoubtedly be worried that the ideal of decentralisation is fast becoming a thing of the past. The Snowden revelations have uncovered an Internet that is highly centralised; a few countries and a handful of private companies have a disproportionate amount of power with regards to its architecture. The Cambridge Analytica[68] debacle gave us a glimpse into the level of centralisation that private entitites have accumulated.

The study of Internet regulation in the next few years will have to tackle the growing levels of centrality. Many people, including this author, still believe that the distributed and open Internet is a worthy cause to support. Besides the common fear of government presence in online communities, exemplified by the ideology of cyber-libertarianism, we need to take a hard look at the way in which the Internet has become a sizeable business, and how a few companies command a disproportionate amount of power. These companies no longer respond to self-imposed promises not to be evil; their reason for existing is to make a profit.[69] The Snowden revelations have uncovered a public-private conglomerate of gigantic proportions, with the US Government and many US-based companies at the centre. Each new revelation has uncovered layers of collaboration that many suspected, but the reality seems to surpass even the worst conspiracy theories.

Internet regulation theories must tackle these issues head on.[70]

---

[68] C Cadwalladr ‘‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower’ *The Guardian* (18 Mar 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (last accessed 21 June 2018).

[69] See also the discussion of the Cambridge Analytica/ Facebook scandal of 2017–2018 in Lillian Edwards’ contribution to this volume in chapter 3.

[70] In chapter 9 of this book, the editor, Lilian Edwards, picks up this notion of the increasing importance of platforms and intermediaries as nodes of central power on the Internet and the trend towards enrolling them by the threat of regulation as chokepoints, censors or filters for content and online activities.