



2017

## Who Runs the Internet?

Anupam Chander


*Georgetown University Law Center*, [ac1931@georgetown.edu](mailto:ac1931@georgetown.edu)

This paper can be downloaded free of charge from:  
<https://scholarship.law.georgetown.edu/facpub/2508>  
<https://ssrn.com/abstract=4446459>

---

Published in *Research Handbook on the Politics of International Law* (Wayne Sandholtz & Christopher A. Whytock eds., Edward Elgar Publishing 2017), pp. 418-442.

This open-access article is brought to you by the Georgetown Law Library. Posted with permission of the author.  
Follow this and additional works at: <https://scholarship.law.georgetown.edu/facpub>

 Part of the [Intellectual Property Law Commons](#), [International Law Commons](#), and the [Law and Politics Commons](#)

Cite: Anupam Chander, Who Runs the Internet, in Research Handbook on the Politics of International Law, 418-442 (Wayne Sandholtz & Christopher Whytock, eds. 2017)

## Chapter 15

# Who Runs the Internet?

Anupam Chander<sup>1</sup>

## Contents

Introduction .....	1
1 The coming of politics to Internet governance.....	5
2 Multilateral vs. multistakeholder governance .....	9
3 ‘Rough consensus and running code’ .....	15
3.1 The international law of cyberspace ( <i>vel non</i> ).....	16
4 The regime complex in internet governance.....	18
5 Governance disputes on the ground .....	21
6 Conclusion.....	22

## Introduction

There is no single answer to the question of who runs the Internet. Is it the United States, often seen as the hegemon of the Internet, home to so many of the world’s leading Internet enterprises? Is it China, which erects a “Great Firewall” to assert control over the portion of the Internet available in China? Is it the European Union, which extends its power globally through its data protection regime, designating countries as “adequate” or (implicitly) “inadequate” to receive its data? Is it ICANN, the California not-for-profit organization that controls how Internet addresses are allocated? Is it the World Wide Web Consortium, which develops standards for the web’s communication’s protocols? Is it the United Nations, which periodically asserts pressure through organs like the International Telecommunications Union or through international meetings? Is it the World Trade Organization, which regulates the barriers that governments erect against international trade? Is it telecommunications providers such as AT&T and Comcast on whose wires and beams information flows? Is it Facebook,

---

<sup>1</sup> The author thanks Nida Siddiqui for excellent research assistance.

which recently connected a billion people in one day? Is it Google, where the world often begins its search for information?

In reality, all of the above, and many more, can claim a share of Internet governance. This chapter will set out an overview of how the Internet is currently governed, as well as some of the key controversies in both the procedure and substance of Internet governance.

Before we delve more deeply into how the Internet is in fact governed (or not governed, as the case may be), however, it is useful to consider how Internet governance relates to politics more generally. Wayne Sandholtz and Christopher Whytock observe that “[t]here are diverse sites of interaction between law and politics.”<sup>2</sup> This is certainly true of Internet governance, which offers varied interactions between law and politics depending not only on issue area, but also location. In this sense, instead of conceptualizing a uniform global cyberspace, we should imagine a geography of cyberspace. The Internet is indeed a global network and creates a global space for many purposes, yet that network and space remains highly heterogeneous and local.<sup>3</sup>

The Internet you experience depends on where you are. Some of the divergences depend on different conceptions of permissible speech. The political censorship of China and Iran is well-known, for example, with Internet service providers and intermediaries ordered to police banned material. Each country has its own sensitivities about what kind of speech cannot be shared. Thailand famously enforces a lèse-majesté law barring the disparagement of the King, or even, in its most recent invocation, the King’s beloved dog.<sup>4</sup> But content based restrictions are present in the most liberal democracies as well. The United Kingdom, for example, has put in place automatic nationwide pornography filters, from which users can opt out if they so inform their Internet service provider.<sup>5</sup> In the United States, copyright owners zealously send “takedown” notices when they find allegedly infringing material online (interestingly, such notices often have global effect as they are likely to be removed from the platform entirely, not just in the United States, a position consistent with the globalization of copyright through the Agreement on Trade-Related Aspects of Intellectual Property Rights). Most recently, we have seen European courts order Google to remove links from its search services to “inadequate, irrelevant or no longer relevant” factual information about a person

---

<sup>2</sup> Wayne Sandholtz and Christopher Whytock, ‘The Politics of International Law’ this volume.

<sup>3</sup> Anupam Chander, ‘Law and the Geography of Cyberspace’ (2014) 6(1) *The World Intellectual Property Journal* 99, 99.

<sup>4</sup> Thomas Fuller, ‘Thai Man May Go to Prison for Insulting King’s Dog’ *New York Times* (New York, 14 December 2015). (‘In a case brought in a Thai military court, the worker, Thanakorn Siripaiboon, was charged with making a ‘sarcastic’ Internet post related to the king’s pet’).

<sup>5</sup> For a quick summary of Internet pornography laws across the globe, see ‘Legal status of Internet pornography’ Wikipedia <[https://en.wikipedia.org/wiki/Legal\\_status\\_of\\_Internet\\_pornography](https://en.wikipedia.org/wiki/Legal_status_of_Internet_pornography)> accessed 5 January 2016.

unless the information supports a public interest.<sup>6</sup> Influential legal scholars in the United States have called for restrictions on social media in order to curb recruiting by the so-called Islamic State.<sup>7</sup> As nations enforce differing privacy rules, we may experience more services that block access from certain jurisdictions. After Spanish authorities ruled that companies that link to a newspaper article have to pay the newspaper for the link, Google simply shut down its Google News service in Spain.<sup>8</sup> What is legally available varies even across a single country: Illinois, Nevada, and New York have banned fantasy sports gambling, while most other states in the United States have not acted to bar such activity.<sup>9</sup>

Of course, a more fundamental difference between how the Internet is experienced across the world is its ubiquity in certain locales and its rarity in others. Access speeds vary widely, a function of the level of investment in the telecommunications infrastructure. Many African countries are only now beginning to receive multiple routes of access to the global Internet, with new undersea cables laid across oceans. For most people, Internet access comes via the small screen on their telephones, as mobile operators have been quicker to expend the large sums needed to provide Internet infrastructure. Even those with access, however, may face other constraints—very slow networks or the ability to purchase only limited amounts of Internet access. Recently, Facebook slowed the Internet down to 2G at its headquarters for a day, so that its engineers and staff could experience the Internet the way that many in the world receive it. Many websites become effectively inaccessible at 2G speeds. In the future, satellites may democratize access further, providing low cost blanket coverage across entire continents.

The topography of the Internet depends on numerous local, national and transnational factors. Sandholtz and Whytock suggest that in undertaking what they call “mid-

---

<sup>6</sup> Case C-131/12 *Google Spain SL v Agencia Española de Protección de Datos* [2014] ECLI 317.

<sup>7</sup> Erik Eckholm, ‘ISIS Influence on Web Prompts Second Thoughts on First Amendment’ *New York Times* (New York, 27 December 2015) <<http://www.nytimes.com/2015/12/28/us/isis-influence-on-web-prompts-second-thoughts-on-first-amendment.html>> accessed 5 January 2016.

<sup>8</sup> Associated Press, ‘Google Shuts Down News Site in Spain, Blocks Spanish Content’ *SFGate* (San Francisco, 11 December 2014) <<http://www.sfgate.com/business/article/Google-shuts-down-news-site-in-spain-blocks-5951177.php>> accessed 5 January 2016. The Spanish copyright law that prompted Google’s decision seems to have backfired: rather than lead to greater revenues for Spanish publishers, it resulted in a loss of traffic to the publishers’ websites, with accompanying losses in advertising revenues. Joe Mullin, ‘New Study Shows Spain’s “Google Tax” Has Been a Disaster for Publishers’ *arstechnica* (30 July 2015) <<http://arstechnica.com/tech-policy/2015/07/new-study-shows-spains-google-tax-has-been-a-disaster-for-publishers>> accessed 5 January 2016.

<sup>9</sup> Joe Drape, ‘Illinois Says Daily Fantasy Sports Are Illegal’ *New York Times* (New York, 23 December 2015) <<http://www.nytimes.com/2015/12/24/sports/illinois-says-daily-fantasy-sports-are-illegal.html>> accessed 5 January 2016.

range” theorizing, we focus on actors, problems, rules, and institutions. This chapter seeks to begin that inquiry.

Local variations are but a part of the regime complex that governs the Internet, a cobbled together *modus vivendi* that includes a disparate set of corporate, civic, governmental and intergovernmental actors who play a role in governance. Internet governance varies by regime.

We might begin by breaking down Internet governance into half a dozen regimes, though yet more could certainly be identified: (1) the regime that manages domain names and Internet numerical addresses; (2) the regime that manages the communications protocol between computers; (3) the regime that manages the physical communications network spanning countries, oceans, and even space; (4) the regimes that regulate the privacy of information; (5) the regime that regulates the content offered on the Internet; and (6) the regime that governs cybersecurity.<sup>10</sup>

Each expert who answers the question “Who runs the Internet?” will highlight different aspects of governance and select different actors. Posing nearly the same question as this chapter nearly a decade ago in their book, *Who Rules the Internet?*, Jack Goldsmith and Timothy Wu argued for the ultimate primacy of governments. Internet governance depends, they conclude, on the state, or in their words, “heavy reliance on the iron fist of coercive government power.” Indeed, governments have demonstrated that they can, if they wish, assert enormous control over the Internet—from banishing domain names (e.g., RojaDirecta.com, seized for a time by the United States), to prosecuting alleged copyright criminals (e.g., the New Zealand arrest of Kim Dotcom), to widely censoring undesirable political speech (e.g., the so-called Great Firewall of China). And stopping cybercriminals ultimately depends on local police forces arresting the criminals. A multiplex of different governors exercise power in cyberspace. They write, “The success of Internet companies like eBay [and] the success of the Internet itself ... depend on something invisible but essential: public goods like criminal law, property rights, and contract enforcement provided by government.”<sup>11</sup> In emphasizing the nation-state part of the Internet governance story, they sought to counter the early “illusion of a borderless world,” where nation-states no longer mattered. Today, the ubiquity of state

---

<sup>10</sup> One might offer an additional regime—the regime to enforce each of the other regimes—but it seems better to see enforcement as part of the regimes themselves. DeNardis and Raymond offer an alternative (and useful) characterization: ‘One way to understand the Internet governance ecosystem is to divide its main functions into six areas: (i) control of ‘critical Internet resources,’ (ii) setting Internet standards, (iii) access and interconnection coordination, (iv) cybersecurity governance, (v) the policy role of information intermediaries, and (vi) architecture-based intellectual property rights enforcement’. Mark Raymond and Laura DeNardis, ‘Multistakeholderism: Anatomy of an Inchoate Global Institution’ (2015) 7(3) *International Theory* 572, 588.

<sup>11</sup> Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) 140, 182.

interventions into Internet governance is evident—from the United States government’s efforts to surveil Internet activity worldwide in its anti-terror campaign, to Turkey’s censorship of Twitter, to the European Union’s rejection of the existing procedure for the transmission of information to the United States, and to the European Union’s creation of a right to delete information from search results.

Yet, an examination of cyberspace governance shows that both non-state and multilateral actors maintain important governance roles on the Internet. Just as non-state governance regimes rely on the state, states also rely on non-state actors. Goldsmith and Wu are certainly correct that any account must not neglect states, which as they noted, provide the legal foundation for the transactions taking place online—enforcing laws against fraud and protecting property and contract. But a state-centered approach neglects the crucial role played by companies in both establishing their own content rules and enforcing, *vel non*, national rules. It also neglects the role of a multistakeholder Internet governance processes used currently to manage the domain name system and the development of the Internet transmission protocols.

My focus here is on the politicization of the Internet, not what we might describe as the digitization (or Internet-ification) of politics. Archon Fung and coauthors have described different models of how the Internet affects politics (*viz.*, muscular public sphere, here comes everybody, direct digital democracy, truth-based advocacy, constituent mobilization, and social monitoring).<sup>12</sup>

## 1 The coming of politics to Internet governance

Some abhor the insertion of politics into Internet governance altogether—as useful perhaps as politicians proclaiming about physics. Should not we see the Internet as pre-political, post-political, or a-political? There are some that would insist that Internet governance should be left to engineers because only engineers will ensure that the data continues to flow, while politicians will simply exploit the Internet to gain further advantage and cement their power. While there is some truth to this fear, even this “anti-political” model is of course ultimately political—merely grounded in a techno-libertarian politics which prefers a system of self-regulation to rules emanating from the state.

Whatever the motivations of politicians, we should recognize that technologies are inherently political. They enable and disable choices. To reject the politicization of the Internet is to deny that the Internet is inherently political, that it favors some goals and not others. Internet design deeply affects privacy, economic development, speech, censorship, and

---

<sup>12</sup> Archon Fung, Hollie Russon Gilman and Jennifer Shkabatur, ‘Six Models for the Internet + Politics’ (2013) 15 *International Studies Review* 30.

surveillance. Laura DeNardis has shown, for example, how issues of privacy and surveillance are embedded in the design of IPv6, the newest generation of the Internet's protocol.<sup>13</sup> The Internet of 2016, for example, supports extensive expression and challenges government censorship, though surveillance and other developments can upset that result.

Given the Internet's growing importance to our lives, the attention of politicians and judges should come as no surprise. Indeed, it should even be desired, even if "politician" carries a negative connotation in today's climate. Politics is the realm of democratic discourse and debate. If the Internet stands to remake entire industries, from publishing to retail to brokerage, then it would seem appropriate for lawmakers and judges to analyze the appropriate framework for regulating the new economic order. Taxi drivers the world over are increasingly worried about the emergence of an unexpected threat of drivers and consumers connected via an app. Hotels fear the rise of platforms where homeowners and travelers can find temporary housing. And the disruptions seem to have just begun. A popular summation of the radical nature of today's economy goes as follows: "Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate."<sup>14</sup> It is no wonder that governments accustomed to regulating taxis, shops, and hotels are both keen to be involved and at a loss for what to do.

A politics of the Internet is inevitable. Even engineers have to begun to acknowledge how politics can impact what is available on the Internet. In 2015, the Internet Engineering Task Force established a new error code, 451, to indicate that a particular Internet resources was "Unavailable for Legal Reasons." The number was selected to recall the censorship of book burning, with 451 being the temperature at which paper burns according to Ray Bradbury in his novel *Fahrenheit 451*.<sup>15</sup> When a user trying to reach a webpage receives error 451, "an HTTP Status Code to Report Legal Obstacles," she would know that she was being denied information because of censorship. Peter Galison has observed that there are differing historical forms of censorship—Austrian censorship with blackbars over the censored text versus German censorship with the material rewritten to make the censorship invisible to the reader. The new error code allows a user denied access to material know that the denial was based on legal reasons.

---

<sup>13</sup> Laura DeNardis, *The Global War for Internet Governance* (Yale University Press 2014).

<sup>14</sup> Tom Goodwin, 'The Battle is for the Customer Interface' *TechCrunch* (San Francisco, 3 March 2015) <<http://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/#.mqkyfmm:0sCd>> accessed 5 January 2016.

<sup>15</sup> Andrew Coust, 'Googler Proposes "451" Error Code to Signal Internet Censorship, in Honor of Ray Bradbury' *Digital Trends* (22 June 2015) <<http://www.digitaltrends.com/web/googler-proposes-451-error-code-to-signal-internet-censorship-in-honor-of-ray-bradbury>> accessed 5 January 2016.

Some will worry that to recognize the political nature of Internet governance is to license outrageous power grabs online. However, the fact that a technology is political does not mean that any political effort to control or reshape it is thereby legitimate. That would be like declaring politics inappropriate for governing a country because some might manipulate politics to oppress a minority group.

The central political dispute with respect to Internet governance is the process by which it should be governed, a question to which we now turn.

*National Digital Sovereignty versus a Global Internet*

Whereas countries may once have seen the Internet as entirely foreign and outside their domain, the politicization of the Internet has grown dramatically in recent years. No longer content to stand on the sidelines of Internet policy-making, countries are becoming more assertive with respect to the Internet. National politicians have sought greater control over the Internet largely because of three developments. First, countries increasingly seek to grow a digital economy, and thus seek to fashion policies that they believe will grow domestic businesses. Second, the fact that foreign media is less susceptible to governmental pressures than local media has made many governments eager to control Internet activities that might otherwise elude local censors. Third, in the wake of the revelations by Edward Snowden and others of widespread digital surveillance by the United States and other countries, governments seek to gain greater control of Internet activities, at times with the unstated goal to increase local surveillance while decreasing surveillance by foreigners.

Russia epitomizes especially the latter two justifications. In 2013, Sergei Zheleznyak, a member of the ruling United Russia party and deputy speaker of the lower house of parliament, declared that Russia needed to reclaim its “digital sovereignty” in the wake of the Snowden revelations.<sup>16</sup> “The Americans ... stick their noses into the personal correspondence of tens of millions of Russian citizens,” he wrote. Two years later, Russia acted to require that foreign companies keep a copy of information about Russian citizens in Russia. Interestingly, the law does not explicitly bar the transfer of personal information overseas, so that one could transfer a copy of the information abroad, as long as a copy were also stored locally.<sup>17</sup> This suggests that the ultimate aim is not diminishing surveillance by foreign countries, but rather enhancing surveillance by Russia. Indeed, the Russian government has proved ruthless in attacking dissidents. 2015 concluded with a Russian court sentencing a blogger to five years in

---

<sup>16</sup> Miriam Elder, 'Russia Needs to Reclaim its “Digital Sovereignty” from US, says MP' *The Guardian* (London, 19 June 2013) <<http://www.theguardian.com/world/2013/jun/19/russia-digital-soveriegnty-nsa-surveillance>> accessed 5 January 2016.

<sup>17</sup> 'Russia Data Localization Requirement at a Glance: Practical Aspects' *Bryan Cave Data Matters* <<http://bryancavedatamatters.com/wp-content/uploads/2015/05/Russia-Data-Localization-Requirement-at-a-Glance.pdf>> accessed 5 January 2016. I am indebted to my student Anna Eck for discovering this fact upon reviewing the Russian text of the law.



prison “for what it said was his extremist activity on the Internet after he urged people to attend a protest against high transport fares and criticized Russian intervention in Ukraine.”<sup>18</sup> Having described the Internet as a “C.I.A. project,”<sup>19</sup> Vladimir Putin seeks now to make the Internet serve his own government’s goals.

Concerns over asserting digital sovereignty are not confined to illiberal regimes. Some in the developing world worry about the possible reemergence of colonialism, now in digital form, as foreign enterprises dominate digital space.<sup>20</sup> Nowhere are these concerns expressed more pointedly than in Europe. The European Union has repeatedly insisted that American Internet companies must follow its dictates. European leaders argue that “the EU has surrendered ground to non-EU-based digital superpowers and essentially forfeited its digital independence.”<sup>21</sup> Europe thus seeks to establish a “Digital Single Market” that will encourage the development of European digital enterprise. According to the European Commission, “achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally.”<sup>22</sup> France’s telecommunications’ authority, the *Autorité de Régulation des Communications Électroniques et des Postes*, declares its desire to promote “digital sovereignty,” a principle that it believes requires foreign communications’ providers to abide by local laws.<sup>23</sup> In Germany, revelations of American spying on the Internet have also led to calls for “digital sovereignty,”

---

<sup>18</sup> Reuters, ‘Russian Court Jails Blogger for Five Years for Extremist’ Posts’ *New York Times* (New York, 30 December 2015) <<http://www.nytimes.com/reuters/2015/12/30/world/europe/30reuters-russia-blogger.html>> accessed 5 January 2016.

<sup>19</sup> Masha Lipman, ‘Putin’s Fear of the Internet’ *The New Yorker* (New York, 25 April 2014) <<http://www.newyorker.com/news/news-desk/putins-fear-of-the-internet>> accessed 5 January 2016.

<sup>20</sup> Prabir Purkayastha, ‘Modi’s Silicon Valley Visit: Inviting Digital Colonialism for Media Hype’ *Newslick.in* (3 October 2015) <<http://newslick.in/india/modis-silicon-valley-visit-inviting-digital-colonialism-media-hype>> accessed 5 January 2016.

<sup>21</sup> Alistair Maughan and Dom Rothbarth, ‘The EU’s Digital Single Market Announcement – Regaining Europe’s Digital Sovereignty?’ *Mondaq USA Business Briefing* (25 May 2015) <<http://www.mondaq.com/unitedstates/x/399040/international+trade+investment/The+EU+Digital+Single+Market+Announcement+Regaining+Europes+Digital+Sovereignty>> accessed 5 January 2016.

<sup>22</sup> European Commission, ‘Digital Single Market: Bringing Down Barriers to Unlock Online Opportunities’ <<http://ec.europa.eu/priorities/digital-single-market>> accessed 5 January 2016.

<sup>23</sup> *Autorité de Régulation des Communications Électroniques et des Postes*, ‘Digital Sovereignty’ (2015) <[http://www.arcep.fr/fileadmin/reprise/communiqués/communiqués/2015/2015-02\\_CNNum\\_ARCEP\\_souverainete\\_numerique\\_VA.pdf](http://www.arcep.fr/fileadmin/reprise/communiqués/communiqués/2015/2015-02_CNNum_ARCEP_souverainete_numerique_VA.pdf)> accessed 5 January 2016; ([T]he obligations contained in national law – particularly with respect to access and interconnection, public safety and security (interception of telecommunications, keeping browser histories, site blocking measures) and protecting end users – are applied to electronic communications operators once they operate electronic communications networks on the national territory, or provide users in France with electronic communications products and services’).

and even, in the hopes of German industrialists, “an independent infrastructure that is free of reliance on the US.”<sup>24</sup>

As the stakes have grown, there is an increasing turn to politics with respect to the Internet. But legitimate interests in promoting local values or local economies often mix with desires to assert greater control over speech within a country and to surveil dissidents more effectively, as the Russian case demonstrates.

Thus, we are seeing a growing diversity of actors seeking to regulate the Internet. Unsurprisingly then, not only are the actors diverse, so are the rules. Indeed, it may be premature to assert that there are clear rules at all. In lieu of clear rulers and clear rules, Internet regulation creates sites of contestation, requiring highly particularized inquiry. Sandholtz and Whytock articulate what they describe as a “mid-range” approach to theorizing about international law, which seeks to identify the distinct institutional and micro-level factors at work as international law interfaces with politics.

## 2 Multilateral vs. multistakeholder governance

Before we decide the rules to govern the Internet and before we even decide what institutions should govern the Internet, we need to determine the types of entities that should be involved in global Internet governance. Here there is a significant divide. Some have argued that the Internet should be governed through some kind of international treaty between national governments, likely administered through the United Nations. Others prefer that Internet governance be conducted through a “multistakeholder” process, which includes governments, the corporate sector, and civil society organizations, all participating as rough equals.<sup>25</sup>

The United States was an early champion of non-government-based models of Internet governance, declaring that it would avoid strict national assertions of control. President Bill Clinton, in a 1997 Memo on Electronic Commerce, declared that “the Federal Government should refrain from imposing new and unnecessary regulations.”<sup>26</sup> He announced, “[T]he private sector must lead.” This meant that “the Federal Government should encourage industry self-regulation wherever appropriate and support private sector

---

<sup>24</sup> Hilmar Schmundt and Gerald Traufetter, 'Digital Independence: NSA Scandal Boosts German Tech Industry' *Speigel Online International* (4 February 2014) <<http://www.spiegel.de/international/business/german-it-industry-looks-for-boom-from-snowden-revelations-a-950786.html>> accessed 5 January 2016.

<sup>25</sup> For an early academic embrace of the multistakeholder model, at least as applied to international meetings, see Joel R. Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review* 1315, 1358.

<sup>26</sup> President William J. Clinton, 'Memorandum on Electronic Commerce' (White House 1 July 1997) 1008.

efforts to develop technology and practices that facilitate the growth and success of the Internet.”

The idea of American values to be conveyed in cyberspace was explicit even here. Even if the U.S. government was not calling the shots, it hoped that the private sector would abide by American values as it developed the Internet. Consider Vice President Al Gore’s exhortation: “I call on the private sector to lead the way – tempering action with wisdom, private gain with the public interest, and wonders yet to come with the values Americans hold dear.”<sup>27</sup> Indeed, the Internet proved a tremendous boon to a prominent American value—robust free expression.<sup>28</sup>

The Clinton Administration made good on its promise to support private sector leadership. First, the United States privatized the parts of the Internet backbone that it had helped to fund, “reshaping the National Science Foundation Network (NSFNET) into what is known today as the Internet.”<sup>29</sup> Second, rather than following the Europeans in establishing a new comprehensive privacy law for the age of computing, it supported private sector privacy initiatives, backed by the Federal Trade Commission’s administrative and civil sanction powers. Third, the United States moved the management of the domain name system to a newly created not-for-profit corporation, the Internet Corporation for Assigned Numbers and Names (ICANN). In 1998, the National Telecommunications and Information Administration<sup>30</sup> announced that “the U.S. Government is prepared to recognize, by entering into agreement with, and to seek international support for, a new, not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system.”<sup>31</sup> It solicited the creation of ICANN, and vested domain name management within it via contract in 1998. Both of the latter two decisions remain controversial even today.

United States leadership in Internet governance was due in large part to the fact that the earliest foundations for the Internet protocols were laid in the United States, often out of government-sponsored activities. The language of interconnection, which came to be known as the Transmission Control Protocol/Internet Protocol, developed largely in the United States. Consider the first map of computers connected to the predecessor to the Internet—the

---

<sup>27</sup> President William J Clinton and Vice President Albert Gore Jr, ‘A Framework for Global Electronic Commerce’ (Letter, White House 1 July 1997).

<sup>28</sup> Anupam Chander and Uyen P Le, ‘Free Speech’ (2015) 100 Iowa Law Review 501.

<sup>29</sup> Rajiv C Shah and Jay P Kesan, ‘The Privatization of the Internet’s Backbone Network’ (2007) 51 Journal of Broadcasting and Electronic Media 93.

<sup>30</sup> The National Telecommunications and Information Administration (NTIA), formed in 1978, is an agency within the United States Department of Commerce.

<sup>31</sup> United States Department of Commerce National Telecommunications and Information Administration, ‘Management of Internet Names and Addresses’ (1998) 63 (111) Federal Register 13741.

ARPANET, from December 1969.<sup>32</sup> On the map are four nodes, the University of California, Santa Barbara, the University of California, Los Angeles, Stanford Research Institute, and the University of Utah. This network was the result of a collaboration between these institutions and the Department of Defense's Advanced Research Projects Agency. The ARPANET was the first network to implement the Transmission Control Protocol/Internet Protocol (TCP/IP).

But the Internet soon burst national walls—growing dramatically across the world. The invention of the World Wide Web in 1990 by a British mathematician (Tim Berners-Lee), who was working for a European laboratory in Geneva, accelerated the pace of Internet adoption dramatically. It was thus natural to expect demands for a greater role in Internet governance from outside the United States.

Global Internet governance discussions heated up in the run up to the World Conference on International Telecommunications (WCIT) held in 2012 in Dubai. As some scholars have written, “The meeting was designed to review and update the International Telecommunication Regulations, a global set of rules governing the exchange of telecommunication traffic across national borders. Administered by the International Telecommunication Union (ITU), the telecom interconnection rules were previously updated in 1988 prior to Internet commercialization and the development of the Web.”<sup>33</sup> In 2011, prior to WCIT, India called for Internet governance to be brought under United Nations control.<sup>34</sup>

The concept of multistakeholder Internet governance was first embraced in a major international forum at the World Summit on the Internet Society, which was convened by the United Nations in 2005 through a General Assembly Resolution adopting a proposal of the Secretary-General of the International Telecommunication Union.<sup>35</sup> Under the banner of the United Nations, the summit committed to a Tunis Agenda for the Information Society, which including the following principle: “We seek to improve the coordination of the activities of international and intergovernmental organizations and other institutions concerned with Internet governance and the exchange of information among themselves. A multi-stakeholder

---

<sup>32</sup> F Heart, A McKenzie, J McQuillan and D Walden 'A History of the ARPANET: The First Decade' (Report No. 4799, Bolt, Beranek and Newman, 1981) fig III-79 <<http://som.csudh.edu/cis/lpress/history/arpamaps/press.jpg>> accessed 5 January 2016.

<sup>33</sup> Samantha Bradshaw and others, 'The Emergence of Contention in Global Internet Governance' (2015) 17 Global Commission on Internet Governance <<https://www.cigionline.org/sites/default/files/no17.pdf>> accessed 5 January 2016.

<sup>34</sup> Joe Waz and Phil Weiser, 'Internet Governance: The Role of Multistakeholder Organizations' (2001) 10 Journal on Telecommunications and High Technology Law 331, 332.

<sup>35</sup> UNGA Res 56/183 (31 January 2002) UN Doc A/RES/56/183.

approach should be adopted, as far as possible, at all levels.”<sup>36</sup> But who were the multiple stakeholders to be included? The Tunis Agenda declared that Internet governance should involve governments, the private sector and civil society (paragraph 34), as well as intergovernmental and international organizations (paragraph 35 (d), (e)) and include the contributions by the academic and technical communities (paragraph 36). But the commitment was somewhat equivocal, in tension with another enunciated principle: “The international management of the Internet should be *multilateral*, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations.”<sup>37</sup> The latter language seemed to contemplate an intergovernmental approach to decision-making, where those in civil society or the private sector could only provide input but not actually make decisions.

The issue of whether the Internet should be governed through a multilateral institution created through the agreement of nation-states or through a looser multistakeholder process has recurred. Over the last decade, however, international support for multistakeholderism for Internet governance has grown. Mira Burri notes that Internet “[g]overnance models have in general become less state-centered.”<sup>38</sup>

Developing countries that were initially skeptical came to endorse the multistakeholder model. In 2014, Brazilian President Dilma Roussef hosted NetMundial, the Global Multistakeholder Meeting on the Future of Internet Governance, which was held in Sao Paulo, Brazil.<sup>39</sup> NetMundial concluded with a statement endorsing multistakeholderism:

Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and the users.<sup>40</sup>

Another important endorsement came from India, as India’s Minister of Communications and Information Technology Ravi Shankar Prasad announced in June 2015 India’s support for the multistakeholder model of Internet governance, during the opening ceremony of

---

<sup>36</sup> World Summit on the Information Society ‘Tunis Agenda for the Information Society’ (Tunis, Tunisia 18 November 2005) WSIS-05/TUNIS/DOC/6(Rev. 1)-E para 37.

<sup>37</sup> *ibid* para 29 (emphasis added).

<sup>38</sup> Mira Burri, ‘The International Economic Law Framework for Digital Trade (2015) 135(2) *Zeitschrift für Schweizerisches Recht* 10.

<sup>39</sup> Marilia Maciel, Nicolo Zingales and Daniel Fink, ‘NoC Internet Governance Case Studies Series: The Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial)’ *Network of Centers* (1 January 2015) <<http://networkofcenters.net/research/internet-governance>> accessed 5 January 2016.

<sup>40</sup> NETmundial Initiative, ‘Principles’ <<https://www.netmundial.org/principles>> accessed 5 January 2016.

ICANN's 53<sup>rd</sup> public meeting in Buenos Aires. He declared, "The Internet must remain plural. It must be managed by a multistakeholder system." He continued, "Not only do we support multistakeholderism, but also we encourage multistakeholderism itself to embrace all geographies and all societies. We will partner with you all to make this a reality. We must work toward this new form of digital democracy." Of the large non-Western countries, China remains perhaps the most skeptical of multistakeholderism, along with Russia.

After some initial equivocation, the European Union has also endorsed multistakeholder Internet governance.<sup>41</sup> The European Commission declared that it is "firmly committed to the multistakeholder model of Internet governance." At the same time, the Commission called upon stakeholders "to further strengthen the sustainability of the model by making actors and processes more inclusive, transparent and accountable."

Why have states refused to enter into an international treaty to govern the Internet? This is a counterpart to the foundational international law question of why states enter into international treaties.<sup>42</sup> Let us examine the question from the perspective of the United States, the country which has remained at all times the principal champion of the multistakeholder model, and thus skeptical of an international treaty. The answer may involve a range of high international law theories. Certainly, the United States government seems to believe that it is in the interest of the United States to continue the current multistakeholder model as U.S.-based Internet enterprises have flourished under it. But even if that is the United States government's private position, its public position is that multistakeholderism is good for all countries because that approach best protects a free and open Internet. But what of the European Union and developing countries, which seem to have moved from demanding an international treaty arrangement for Internet governance to a less defined multistakeholder process? Indeed, if the realist view is correct, then it is unclear why countries have come to change their position on this key point. Did their interests change, or did they reconsider what international arrangement would best serve them? Seemingly essential to this process are transnational norm entrepreneurs consisting of Internet activists from across the world who have promoted the vision of Internet governance as a shared enterprise among both state and non-state actors.

The United States arrangement with ICANN rested for a long period on a contract between the United States Department of Commerce and ICANN. This suggested that ultimate authority was retained by the United States government, as it could revoke ICANN's authority. Single country control over the basic domain name and numerical address function of the Internet is contrary to a multistakeholder process, and thus the United States could not

---

<sup>41</sup> Commission, 'Internet Policy and Governance Europe's Role in Shaping the Future of Internet Governance' (2014) <<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0072>> accessed 12 January 2016.

<sup>42</sup> In their introduction, Sandholtz and Whytock cite a number of studies (including the work of Oona Hathaway) examining why states enter into international treaties.

simultaneously promote multistakeholderism while insisting on ultimate single country control over this basic function. Accordingly, due to international pressure arising from this inconsistency, the United States has moved cautiously to yield control over ICANN. On the eve of NETmundial, the NTIA announced that the United States would “transition oversight to the multi-stakeholder community by 2015.”<sup>43</sup> Even though ICANN was founded through a grant of authority by the United States Department of Commerce, today ICANN claims a global authority stemming from its multistakeholder governance model. Perhaps uniquely for a body with such global significance, ICANN remains a California not-for-profit corporation.

Multistakeholderism is no magic talisman guaranteeing representation, accountability, and responsibility.<sup>44</sup> Some criticize the operation of the multistakeholder model today in Internet governance, pointing out that ICANN discussions are neither truly global nor multistakeholder, being dominated by Western countries and corporate interests.<sup>45</sup> Given that the Internet is increasingly used by people outside the West, this is a serious criticism. Internet scholar William Dutton has noted that “forty-five percent of the global Internet population is in Asia and the Pacific.”<sup>46</sup> Dutton continues, “For example, there are more Internet users in China, than there are Americans on the planet. In short, the Internet is no longer a North American and European technology. It is increasingly global.” It is essential that all the people in the world have a voice in how the Internet is governed.

Of course, the difficulty of bringing developing countries into global governance processes is not unique to Internet multistakeholderism. Even multilateral United Nations institutions have long faced this challenge. UN institutions have adopted a variety of steps to mitigate this problem. In some, leadership might rotate by convention across geographic areas. This is true of the United Nations’ highest post, the Secretary General. Efforts to include the developing world go beyond the top leader to the UN staff itself. Citizenship is a key criterion for many UN staff positions, as the UN seeks to operate through a broadly representative workforce. Many UN institutions perform their work in multiple official languages. Many UN institutions offer special training to persons from the developing world in order to build capacity—though one has to be careful that such “capacity building” exercises are not a simply a cover for promoting the interests of developed countries.

---

<sup>43</sup> Bradshaw and others (n 33).

<sup>44</sup> Waz and Weiser (n 34) (asking whether multistakeholder organizations ‘are truly representative, accountable, and responsible’).

<sup>45</sup> Pranesh Prakash, ‘The “Global Multistakeholder Community” is Neither Global Nor Multistakeholder’ *Centre for Internet & Society* (20 October 2015) <<http://cis-india.org/internet-governance/blog/global-multistakeholder-community-neither-global-nor-multistakeholder>> accessed 5 January 2016.

<sup>46</sup> William H Dutton, ‘Multistakeholder Internet Governance?’ (2015) <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2615596](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615596)> accessed 5 January 2016.

### 3 ‘Rough consensus and running code’

Borrowing from computer engineers, the Internet communications model can be described in terms of layers, with the number and content of layers depending on the particular implementation and characterization. European scholar Mira Burri breaks Internet communications down into three layers, which proves especially useful to legal scholars. They are: (i) the physical layer consisting of the real world communications network of switches, cables, computers, and other hardware devices; (ii) the logical layer consisting of software, applications and protocols; and (iii) the content layer, where the actual human readable messages are placed.<sup>47</sup> Even though governments are ultimately concerned most about the content layer (to which we turn in the section later in the chapter detailing two disputes about Internet content), the official struggles between multistakeholderism and multilateralism have largely been about the governance of the logical layer—the software mechanics that keep the Internet running. It is useful then to examine the governance of this layer a bit more closely.

It may be hard to imagine that such a diverse group of entities of varying sizes and power would be able to reach decisions. Often, multistakeholder organizations function on the basis of a “rough consensus.” Rough consensus replaces both a top-down and a one-person-one-vote simple majority rules arrangement. A top-down approach is hard to obtain when it comes to Internet governance because there is simply no authority that governs what rules computers must use in talking to each other. At the same time, a simple majority based approach is also ill-suited because of the varying sizes and authoritativeness of the players.

Thus, in the words of Internet pioneer David Clark in 1992, “We reject: kings, presidents, and voting. We believe in: rough consensus and running code.” That described the decision-making model of the Internet Engineering Task Force (IETF), which developed the protocols that govern the Internet.<sup>48</sup> The working groups of the IETF operate on this basis, with “rough consensus” translating to a “very large majority of those who care must agree.”<sup>49</sup> Rough consensus would be hammered out through documents known as Requests for Comments (RFCs), circulated through the community to develop new standards for networking. As Internet pioneer Vint Cerf observes, “The RFCs document the odyssey of the ARPANET and, later, the Internet, as its creators and netizens explore, discover, build, rebuild, argue and resolve questions of design, concepts and applications of computer

---

<sup>47</sup> Burri (n 38).

<sup>48</sup> Andrew L Russell, ‘Rough Consensus and Running Code and the Internet-OSI Standards War’ (2006) 28(3) IEEE Annals of the History of Computing 48, 48.

<sup>49</sup> Paul Hoffman, ‘The Tao of IETF: A Novice’s Guide to the Internet Engineering Task Force’ *The Internet Engineering Task Force* (2 November 2012) s 4.2 <<https://www.ietf.org/tao.html#getting.things.done>> accessed 5 January 2016.



networking.”<sup>50</sup> Today, the IETF is one of the bodies operating under the auspices of the Internet Society, as is the Internet Architecture Board.

What is often lost in the celebration of the Internet’s success is the fact that all along, the Internet’s governance model grew in the face of competition. In France, there was the Minitel, a national network built out through the phone network. Minitel represented a top-down approach to the problem of computer networking, “the product of French government central planning—*dirigisme*—aimed at forestalling American domination of the information and communication technology market in France.”<sup>51</sup> A more international competitor was the Open Systems Interconnection (OSI) standard, which was developed through the international standards-setting body ISO, in collaboration with the International Telecommunications Union.<sup>52</sup> Given that there was no global authority to mandate any particular standard, for any particular standard to flourish, it had to find institutions and individuals who would adopt it. The IETF approach proved the most successful in achieving widespread adoption, in part because it had a head start over the others. As Vint Cerf notes, “[T]he Internet Engineering Task Force [evolved] from just one of several task forces whose chairpersons formed the Internet Activities Board to the dominant, global Internet Standards development organization, managed by its Internet Engineering Steering Group and operating under the auspices of the Internet Society.”<sup>53</sup>

### 3.1 The international law of cyberspace (*vel non*)

Not only are the actors who regulate cyberspace myriad and varied, the law of cyberspace is as well. Indeed, it is difficult to identify an international law of cyberspace. The Internet is an increasingly global communications network, with some three billion users around the world. But that network does not have a single, consistent set of rules.

In his remarks entitled “International Law in Cyberspace,” leading international lawyer Harold Koh does not purport to offer a special international law of cyberspace—but rather the application of traditional international law to the domain.<sup>54</sup>

What should an international law of cyberspace look like, should one be created? Molly Land argues that an international law of the Internet should be developed from Article 19 of the International Covenant on Civil and Political Rights, which provides: “Everyone

---

<sup>50</sup> Vint Cerf, RFC Editor and others, ‘30 Years of RFCs’ (The Internet Society 7 April 1999) s 4, 4 <<https://www.ietf.org/rfc/rfc2555.txt>> accessed 5 January 2016.

<sup>51</sup> Lyombe S Eko, *New Media, Old Regimes: Case Studies in Comparative Communication Law and Policy* (Lexington Books 2012) 214.

<sup>52</sup> Russell (n 48) 52. See also *ibid* 59 fn 43.

<sup>53</sup> RFC Editor and others (n 50).

<sup>54</sup> Harold Hongju Koh, ‘International Law in Cyberspace’ (2012) 54 *Harvard International Law Journal* 1.

shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.”<sup>55</sup> As Land argues, this modern human rights was developed to apply “technology that had yet to be invented.”

There is much to commend a free expression approach to Internet governance. The Internet is first and foremost a technology of communication, though it is rapidly developing into more. Yet, the difficulty with a free expression-based approach is that it doesn’t answer the difficult questions that inevitably arise when different values come into conflict with free expression. China, for example, declares itself a champion of free expression online: “Chinese citizens fully enjoy freedom of speech on the Internet.”<sup>56</sup> Of course, at the same time, the Chinese microblogging site Sina Weibo “reportedly hired over 1,000 people to manually monitor and delete posts around the clock in addition to auto-filtering.”<sup>57</sup>

Even defining the Internet becomes ever more complicated as the years pass. In 1996, we could define the Internet as “the international computer network of both Federal and non-Federal interoperable packet switched data networks.”<sup>58</sup> The idea of a “Federal” data network had become obsolete even in 1996, as the federal government had already privatized the Internet backbone in the United States in the previous two years. The Internet Tax Freedom Act, 47 U.S.C. Code § 151 (c) offers the following definition:

The term ‘Internet’ means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.

For its part, the Communications Act of 1934, 47 U.S.C.A. § 231(e)(3), offers the following variation:

The term “Internet” means the combination of computer facilities and electromagnetic transmission media, and related equipment and software, comprising

---

<sup>55</sup> Molly Land, ‘Toward an International Law of the Internet’ (2013) 54 (2) Harvard International Law Journal 393.

<sup>56</sup> Information Office of the State Council of the People’s Republic of China, ‘White Paper’ *China.org.cn* (Beijing, 8 June 2010) art III  
<[http://www.china.org.cn/government/whitepaper/node\\_7093508.html](http://www.china.org.cn/government/whitepaper/node_7093508.html)> accessed 12 January 2016.

<sup>57</sup> Min Jiang, ‘Chinese Internet Business and Human Rights’ (2016) 1(1) Business and Human Rights Journal 139, 140.

<sup>58</sup> Communications Decency Act [1994] 47 US Code s 230(f).

the interconnected worldwide network of computer networks that employ the Transmission Control Protocol/Internet Protocol or any successor protocol to transmit information.

Even this depiction seems increasingly quaint, as the Internet seeps ever more deeply into our lives, our constant companion in the form of a smartphone, and increasingly embedded in the physical objects that surround us. The Internet has burst from the boundaries of computers, now intermediating and resolving our interactions with the physical world. The days of dial-up and Internet connections that took work and often generated aggravation are increasingly disappearing for those on the lucky side of the Digital Divide. The Internet is, in this sense, no longer readily separable from the real space. Thus, the question of who rules the Internet becomes increasingly intertwined with all other regulation. That said, there are governance issues that require an understanding of the particular history and characteristics of the Internet.

It is important not to conflate the Internet with the World Wide Web. The Web is one merely application of the Internet, a particular way of sharing information using the Internet Protocol. While groups such as the Internet Society (and its related entities) develop Internet standards, the World Wide Web Consortium, which includes the Web's original author, Tim Berners-Lee, manages the development of Web protocols, though it lacks any official mandate or power that would enable it to simply impose its rules across the Web.

The rise of mobile computing has led to Internet access being mediated not through the World Wide Web, but through dedicated "apps" that are typically not designed to give access to a broad array of sources of Internet-reachable content. This has led to the concern that individuals' broad Internet access rights may be diminished in favor of individuals being limited to a reduced subset of data accessible through a proprietary app. Specialized apps have proven especially popular in a smartphone environment because smartphones have lack the keyboard and large screen available in the laptop or desktop computer environment. Thus far at least, it seems that individuals enjoy both broad access to the Internet through the browser and the convenience of a specialized app dedicated to certain tasks.

#### 4 The regime complex in internet governance

Not only are we prone to simplifying the Internet's present governance, we often conjure a simple past. The United States government, we often hear, created the Internet. That is only a partial account, as we have seen. The Internet grew in an organic fashion, a cobbling together of national government policies, international treaties, university and corporate innovation. As we have seen, that governance architecture has come to be called the "multistakeholder model," where diverse "stakeholders," including international organizations,

governments, corporations, and civil society groups collaborate, both formally and informally, on governing the global networking infrastructure.

The reality is more complicated still. The lack of a top-down structure means that the Internet is regulated, or not, through a complex of regimes, which include at least the following (as mentioned above): (1) the regime that manages domain names and Internet numerical addresses; (2) the regime that manages the communications protocol between computers; (3) the regime that manages the physical communications network spanning countries, oceans, and even space; (4) the regime that regulates the privacy of information; (5) the regime that regulates the content offered on the Internet; and (6) the regime that regulates cybersecurity.<sup>59</sup>

While multiple stakeholders are involved in various aspects of Internet governance, narrower constituencies have greater influence over each of the different regimes. As Internet scholars Laura DeNardis and Mark Raymond write, “There is no unitary system that oversees and coordinates the Internet.”<sup>60</sup> Some of these issue areas are governed by multistakeholder processes (domain names, Internet numerical addresses, and communications protocols), by multilateral processes (international telecommunications), and by both nation-states and corporations (privacy and content). Thus, while multiple stakeholders together govern the totality of cyberspace, the United Nations, governments, non-governmental organizations, and for-profit corporations take the lead in specific aspects of Internet governance. Recognizing this helps avoid the impression that every governance decision in cyberspace is made through multistakeholder processes, or that such decisions could be turned over to a multilateral process. As DeNardis and Raymond observe, “A question such as ‘who should control the Internet: the United States, the United Nations, or some other entity,’ is incongruous because it inherently assumes that Internet governance is a singular system, and also completely discounts the highly privatized nature of Internet administration.” As scholars including DeNardis and Raymond writing for the Global Commission on Internet Governance note, there is a “complex distributed ecosystem of Internet governance.”<sup>61</sup>

---

<sup>59</sup> Laura DeNardis and Mark Raymond offer a useful alternative division of the Internet governance regime: ‘One way to understand the Internet governance ecosystem is to divide its main functions into six areas: (i) control of ‘critical Internet resources’, (ii) setting Internet standards, (iii) access and interconnection coordination, (iv) cybersecurity governance, (v) the policy role of information intermediaries, and (vi) architecture-based intellectual property rights enforcement’. DeNardis and Raymond (n 10); Joseph Nye also offers yet another useful mapping of the cyberspace regime complex. Joseph S Nye Jr, ‘The Regime Complex for Managing Global Cyber Activities’ (2014) 1 Global Commission on Internet Governance Paper <<https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities>> accessed 5 January 2016.

<sup>60</sup> DeNardis and Raymond (n 10).

<sup>61</sup> Bradshaw and others (n 33).

It thus seems appropriate then to use the term “regime complex” to describe the “loosely coupled set of regimes” that govern cyberspace.<sup>62</sup> As Joseph Nye describes, “While there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.”<sup>63</sup>

The regime complex approach, as Joseph Nye observes, offers “a useful corrective to the usual UN versus multi-stakeholder dichotomy as an approach to cyber governance.”<sup>64</sup> As Laura DeNardis writes, “The appropriate question involves determining what is the most effective form of governance in each specific context.”<sup>65</sup>

The regimes in the issue areas described above are not neatly separable into different issue domains, but rather carry substantial overlaps with each other. Consider the fact that privacy can be affected by choices about the domain name system and authentication schemes in communications protocols and architecture. Some would even prefer content regulation through domain name control—seeking to banish certain content from cyberspace through the deletion of domain names and addresses.<sup>66</sup>

The regime complex for Internet governance includes the World Trade Organization, with its extensive treaty obligations and effective international dispute resolution mechanism. But while they affect Internet governance, the WTO treaties do not purport to offer a comprehensive set of rules for the Internet. Rather, they focus on reducing protectionism. Because online companies offer a variety of services, such as search, advertising, and health monitoring, WTO rules can help to level the playing field for foreign providers of Internet services. In this sense, the WTO rules help keep the Internet global, and resist efforts to Balkanize, or break up, the Internet into zones accessible only to domestic consumers and suppliers. With the prominent exception of intellectual property where the WTO actually sets out a minimum substantive rules that member states must apply, the WTO does not generally mandate the rules governing any particular area of trade.

---

<sup>62</sup> Nye (n 59).

<sup>63</sup> *ibid* 7.

<sup>64</sup> *ibid*.

<sup>65</sup> DeNardis (n 13).

<sup>66</sup> For example, a federal district court in California sought to remove content (specifically, banking information) from the Internet by ordering the deletion of the Wikileaks domain name from the domain name registry. Anupam Chander, *The Electronic Silk Road: How the Web Binds the World Together in Commerce* (Yale University Press 2013). This proved somewhat futile, as news websites, including The New York Times, published the Internet Protocol numerical address of the Wikileaks server in response. Upon widespread criticism of the tactic (and perhaps its apparent futility), the judge quickly reversed his initial order.

## 5 Governance disputes on the ground

While global Internet governance discussions often seem abstract, involving broad principles, it may be useful to examine some narrower disputes that might better provide a sense of the day-to-day questions that arise in global Internet governance. Consider two disputes from December 2015. These demonstrate that ultimately, governments are most concerned about the content lawyer of the Internet.

In Brazil, a São Paulo judge ordered the blocking throughout the country of WhatsApp for a period of two days. The judge did so apparently because the judge believed that WhatsApp had not cooperated in a criminal investigation. Tens of millions of Brazilians who use WhatsApp, a service owned by Facebook, could not use the service until another judge lifted the temporary ban. As the *Wall Street Journal* reported, “The [ban] appeared to be a violation of a Brazilian law passed last year called Marco Civil, which protects websites from bearing responsibility for third-party content and prohibits them from being blocked.”<sup>67</sup> What are WhatsApp’s obligations to respond to orders from judges across the world? What ability should a local judge have to enforce his or her order against a company that runs its operations from a different hemisphere?

Also in December 2015, the Turkish government fined Twitter \$50,000 for refusing to remove content that the government considers “terrorist propaganda.”<sup>68</sup> According to news reports, “Twitter has responded by filing a lawsuit in an Ankara court seeking to annul the fine.”<sup>69</sup> Should Twitter simply conform to demands to remove information based on a single government’s definition of what constitutes support for terrorism?

Questions like these will persist for some time, part of the growing pains of the global interactions made possible within the framework of nation-states. Disputes like these complicate any effort to characterize a multistakeholder model for Internet governance for significant aspects of what happens on the Internet. Even if there are multiple stakeholders involved, they may not be collaborating or competing in any organized governance regime, but rather negotiating on an ad hoc basis.

---

<sup>67</sup> Will Connors and Rogerio Jelmayer, ‘Brazilian Judge Lifts Ban on Facebook’s WhatsApp’ *Wall Street Journal* (New York City, 17 December 2015) <<http://www.wsj.com/articles/brazil-court-suspends-facebooks-whatsapp-for-48-hours-1450348131>> accessed 5 January 2016.

<sup>68</sup> Jessi Hempel, ‘Twitter’s Latest Challenge: Deciding Who’s a Terrorist’ *Wired* (San Francisco, 8 January 2016) <<http://www.wired.com/2016/01/twitters-latest-challenge-is-deciding-whos-a-terrorist>> accessed 12 January 2016.

<sup>69</sup> *ibid.*

## 6 Conclusion

To talk of Internet governance is to embrace messiness. There are a growing number of actors and institutions involved in Internet governance, an increasing range of issues implicated, and growing economic, social and political importance of how the issues are resolved.

Whatever the messiness, the end product is *mirabile visu*. On August 27, 2015, Mark Zuckerberg posted on his Facebook wall: “For the first time ever, one billion people used Facebook in a single day.”<sup>70</sup> He went on, “On Monday, 1 in 7 people on Earth used Facebook to connect with their friends and family.” And he was not done: “[I]t’s just the beginning of connecting the whole world.”

---

<sup>70</sup> Mark Zuckerberg, ‘We Just Passed an Important Milestone. For the First Time Ever, One Billion People Used Facebook in a Single Day’ Facebook (27 August 2015) <<https://www.facebook.com/zuck/posts/10102329188394581>> accessed 5 January 2016.