Authority and Regulation in an Interconnected World

https://www.e-ir.info/2019/12/06/standardizing-authority-and-regulation-in-an-interconnected-world/

P.J. BLOUNT, DEC 6 2019

This is an excerpt from *Reprogramming the World: Cyberspace and the Geography of Global Order*. Get your free copy here.

In 1975, the United States and the USSR launched a space mission to dock an Apollo module with a Soyuz module.[1] The mission was a carefully orchestrated scientific mission that was intended to show how science for peaceful purposes could bridge ideological gaps and to further détente between the two nations. The effectiveness of the mission in political terms is a story for another day. The object here is to draw an insight from a small sidebar of the narrative surrounding the mission. The two states both had their respective docking systems. Each relied on, technically speaking, a female side which received the male side of the docking apparatus, much like a headphone jack. In the tense political atmosphere, neither side wanted to become the female side of the other's docking system. As a result, the two countries developed an androgynous docking system that was interoperable with itself.[2] The point here is not to highlight the misogyny inherent in these terms and Cold War politics, which is a continuation of an international relations discourse that often characterizes dominance as male.[3] Instead, it is to point out that the standardized docking mechanism, which is purely a technical specification, holds a great deal of political content. The standardization creates technical interoperability, but the technical standard is the mediator of state-to-state communication. In the Apollo-Soyuz mission, it was a question of technical connection that defined the parity of the states involved as they brought their quasi-territories into proximity.

Usually, questions of standardization occur when states are already in proximity, and international telecommunication has a long history of international governance mechanisms to develop such standards.[4] The ITU as the world's oldest international organization represents a legacy of international cooperation and coordination on telecommunications standards. It also charts a unique history through which international law was developed in such a way that it avoided sticky issues of content by favoring interconnection over interoperability. States' ongoing ability to negotiate and adopt law in the realm of telecommunications would arguably make the international governance regime well prepared to regulate the Internet and Cyberspace, but this has not been the case. This chapter will investigate this phenomenon and argue that the development of Cyberspace governance has served to delegitimize the state as the central governance actor within the sphere. It will also argue that an important part of this delegitimization is the undermining of consent as envisioned in international law.

To construct these arguments, this chapter will proceed first by examining the nature of the ITU's power to make law and regulation concerning international telecommunications. This section will give a historical overview of the ITU and then investigate the most recent effort by states to extend the ITU's authority over the Internet. The next section will examine the development of global multistakeholder governance through an examination of the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN). The final section will examine the trend of corporate intermediaries in Cyberspace and their capacity as governance bodies.

Harmful Interference

The need to facilitate interconnection among states through telecommunication is as old as the telegraph, and the ITU dates to this period having first been established as the International Telegraph Union.[5] The utility of telegraph technology was immediately apparent, but states wanted to ensure that they controlled the technology as it crossed

their borders. As a result, the ITU began as an organization that developed standards and rules for cross-border telecommunications, which allowed for interconnection among countries. This regime gave states primary control over telecommunications at the nodes where physical infrastructure crossed their borders. Today, the mission of the ITU is "facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunications services."[6]

This strategy worked well with lined communications such as telegraph and telephone, but broadcast brought on new challenges, because radio waves do not conform to state borders. There was, as a result, much debate in the international community on the nature of international responsibility for content crossing borders on radio waves. This can be seen in the Soviet complaints about radio propaganda during the Cold War[7] as well as in the UN General Assembly's controversial adoption of the Direct Broadcasting Principles.[8] The ITU again avoided coming into contact with the issue of content by adopting a policy of coordinating international usage of electromagnetic frequencies by nations so as to prevent harmful interference between broadcasts.[9] More recently, there was a movement in the ITU to give developing states more access to international telecommunications development resources.[10] Of course, in the realm of international relations a state's disbursement of aid is highly attenuated by a state's political goals. The ITU again avoided questions of content by developing a division that advocated for such development, but left the legal substance to bilateral or regional agreements.[11] Held argues that technical international organizations such as the ITU "have been sharply delimited" in order to make them "politically unexceptionable."[12] In the case of the ITU, its actions have been delimited to facilitating interconnection and coordinating usage.

Two key observations need to be made here. First, the ITU is a body made up of states as the basic unit of the body politic,[13] and the ITUs legitimacy, like that of other international organizations, springs from "state sovereignty."[14] Votes in the ITU are allocated one to one, and while non-governmental actors are given access to participate in deliberations,[15] the state is the primary power holder in the ITU forum for international coordination, meaning that the rules that it adopts are manifested through the "filter of domestic structures and domestic norms."[16] The ITU is a treaty-based organization, and as such it springs from within the logic of international governance, which reifies international conceptualization of the world.

Second, the ITU makes international law and policy. The ITU's outputs consist of a variety of law and policy documents. As the international body that adopts the rules of international telecommunication, the ITU adopts resolutions that chart its own course in addressing the issues raised by telecommunication technologies. More importantly, the ITU meets regularly to update the rules that make up the Radio Regulations. The Radio Regulations is a treaty of technical standards that is negotiated among members and sets out the regime for coordination of international radiotelecommunication. The Radio Regulations create international obligations that apply to states, not telecommunication providers, directly. In effect, the ITU depends on the member states to make its rules operable through national regulation binding upon domestic actors. Regulation as a result relies on consent of the state parties to the adopted rules.

As an international lawmaking body with the competency and a proven record for coordinating international telecommunication activities, it would seem that the ITU would be well situated to extend its hand of governance over the Internet, which fits easily within the definition of international telecommunication, which is "[a]ny transmission, emission or reception of signs, signals, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems."[17] The technology involved is exactly the type of technology that the ITU was developed to coordinate across borders, but the ITU has been unable to exert direct control within the sphere of Cyberspace. It has, instead, taken on a role more akin to a stakeholder within Cyberspace governance. This is in part due to the historical conditions that led to the governance of information technologies being "dominated" by other organizations.[18]

This inability of the ITU to effectively extend its competency can be seen in the results of its Plenipotentiary Conference held in Busan, Korea in 2014 (PP-14). This meeting was preluded by media chatter warning of an ITU takeover over the Internet, which taps into an established "media narrative . . . about a possible Internet governance takeover" by the UN.[19] These headlines were prompted by the position being taken by the Russian Federation and

other states that the ITU should have more control over the Internet.[20] The position of this bloc of states was widely interpreted as a threat to a free and open Internet. For instance, the U.S. characterized the proposals as mechanisms "that could have provided a mandate for the ITU in surveillance or privacy issues; inhibited the free flow of data; regulated Internet content and service companies; undermined the multistakeholder process; or called on the ITU to develop international regulations on these issues."[21] There was more to this than just rote suspicion of the UN. As a product of international law, the ITU would need to extend the logic of international governance to Cyberspace to effectively regulate its mechanisms. This would mean adopting measures that allow for cross border interconnection while avoiding embroiling itself into disputes over the content of communications. This would give states the ability to adopt, through the ITU forum, technical standards that facilitate national content controls. Such standards would increase state power to censor, monitor, or treat with deference communications entering their borders.

In Busan, the moves to extend the ITU's competency were defeated through the work of the U.S., which "built a broad consensus that led to success on Internet and cybersecurity issues keeping the ITU's work focused on its current mandate."[22] These efforts served "to mitigate and remove proposed language from resolutions that would have improperly expanded the scope of ITU."[23] The results of the negotiations are a handful of nonbinding resolutions that resemble policy statements.[24] So for instance, Resolution 2 calls for a global framework to exchange information on such technologies to "support the harmonious development of telecommunication services."[25] More strikingly, Resolution 101 gives direct recognition to IGCs by "requesting" the Standardization Sector to continue "collaborative activities on IP-based networks with ISOC/IETF and other relevant recognized organizations."[26] The ITU further adopted Resolution 102, which states that "management of the Internet is a subject of valid international interest and must flow from full international and multistakeholder cooperation."[27] This resolution seemingly cedes power to an ambiguously defined "multistakeholder" system, which will be argued below exists outside the bounds of international legal geography.

Trading off coordination for content is, of course, the status quo of international telecommunications regulation, which raises the question of why Internet technology has resisted the encroachment of international law from the exact international body charged with regulating that type of technology. A simple answer would be that states simply do not want to extend international law to govern Cyberspace, and to some extent this is true. However, it seems odd that Cyberspace has such a prominent role in social life at the global level, and that international law remains largely silent on the matter. To be clear, it is not that states are disinterested in the Internet – it is clearly an item on the agenda of the international community. Yet, it is one that international governance is at a loss to comprehensively address. A more satisfying answer can be found in the geography of Cyberspace that exists outside the logic of international geography. Critically, the legal geography of Cyberspace is built around code which is both content and medium. As a result, the "sharply delimited" functions of the ITU are ill equipped to expand to control a medium that is concurrently content. The state is not deprived of jurisdiction completely, as should be obvious from existing domestic laws, but those laws can only extend to the layers of Cyberspace that intersect national space. As a result, international governance has lost significant control over transnational communication, which no longer conforms to the bordered assumptions that underlie international governance.

This does not mean that Cyberspace is without authority. It means that the state becomes one of many stakeholders in a multistakeholder legal geography. The next two sections will investigate the trend of global multistakeholder governance by first examining the technical bodies that govern the logical layer of the Internet and then through analysis of corporate and commercial interests that extend governance over the Internet. These sections together reveal a world-scale legal geography that is not dominated by the state. It is most certainly not devoid of the state, but the state is no longer the central node of authority and need not consent to these governance mechanisms. This is a critical problem for international governance since it is based on a model in which the state is the primary authority.

Rejecting Kings

"We reject kings, presidents and voting" is a phrase worthy of most fringe political manifestos. Though dripping with anti-authoritarian angst, the phrase is not from The Anarchist's Cookbook. Instead, it is found in the central

document, "The Tao of the IETF," that explains the workings of the Internet Engineering Task Force (IETF).[28] This is the technical body that adopts standards that govern the logical layer of the Internet. The statement is more than one of personal rejection of the authority; it is a community rejection of state authority over the methods and means of communication, specifically within the geography of Cyberspace.

The rejection of kings has strong roots in the anarcho-libertarian tradition of many coders who were instrumental in developing the Internet as discussed in Chapter 4. While the rhetoric used is anarcho-libertarian, this statement is not a simple denial of state authority. It is in practice an assertion of authority beyond states, which is consistent with the ITU's inability to extend its own mandate. Multistakeholder governance structures remove the state's ability to dominate regulatory decisions by removing the state's ability to consent to governance. Consent to the law by states is a bedrock principle in the international legal system. States, however, do not have the ability to consent to new standards in Cyberspace. In the multistakeholder model "[t]here is no geographically localized set of constituents" with a claim to legitimacy to deploy power.[29] Legitimacy, as a function of consent, has been redistributed from communities defined by borders to "the participants themselves," and they could be anywhere.[30] The borders of the state do not define the political community of Cyberspace, which disaggregates the core unit of international geography.[31] The legal geography of Cyberspace is not bordered. It is coded, and code is law.[32]

The IGCs discussed briefly in Chapter 2 are representative of the multistakeholder governance that diminishes a state's power to consent to law. The IETF serves as a perfect example and its actions can be seen to push its authority over states. This multistakeholder body adopts and maintains the standards that make the Internet work, including the TCP/IP, and it has the "largest influence on the technologies used to build the Internet."[33] TCP/IP is exactly the type of code that rejects kings, and it gives the IETF "a powerful seat of authority."[34] These protocols move activity to devices at the edges of the networks, which gives the user any freedom that he or she can program into Cyberspace. The state's bordered control points become null when data can move through any connection, thereby jumping those borders. Importantly, states never consented to this, whereas they did consent to telephone lines crossing their borders and to the standards for interconnection promulgated by the ITU and to the frequency allocations governing terrestrial and space-based broadcast technologies. They even agreed over how postal services will be exchanged between them. However, they never agreed on the TCP/IP, which transforms other telecommunication technologies. The natural choke point found at the border fragments when information fragments through packet switching. Even physical gaps are becoming less effective as can be seen by Stuxnet, which jumped an air gap, as well as in projects that seek to get electronic devices across the border of states like North Korea.[35]

The IETF evolved out of the historical development of the Internet in which the computer scientists using the Internet were also making decision about how that space would be constructed.[36] As a result, decision making evolved from group conversations among the coders. The IETF was born from these conversations, which were extraneous to the state, and thus states were never admitted to the decision-making process. As the Internet grew, so too did the IETF. It eventually opened its membership to anyone that wanted to join and take part in that decision-making process. It was community governance built on "rough consensus and running code."[37] This form of decision-making added decisional value to the functionality of code in addition to the value of consensus. This is important because for standards to be effective they must be widely accepted."[38] States may have agents join to represent their respective interests, but these individuals are on equal footing with a variety of others including corporate agents and civic minded netizens. This removes the state from the dominant position it holds in international governance. The IETF's open and transparent process creates interoperability standards that shape the "modern public sphere and broader conditions of political speech."[39] This means that the IETF structures the discursive space within states and without their consent.

The IETF makes decisions on how data will travel across borders outside the scope of the state, but significantly, it "has no formal authority over anything but its own publishing process,"[40] and its status is further complicated by the fact that it has "no formal membership."[41] The decisions that it takes construct the logical layer of the Internet, and state power in that decision process is limited to the ability to send representatives. The state, in the formal sense, is never consulted on IETF decisions, which erodes the state's ability to consent to rules governing transnational communications. This is a significant development in governance at a world-scale and should not be downplayed. The spatial settlement premised on sovereign equality is, in essence, challenged by a set of rules that recode borders

in such a way that states lose significant control over the flow of information across them. This is further confirmed by the IETF's lack of legal personality.[42] This feature means the IETF exists outside of the jurisdiction of any state. The IETF's organizational nebulousness resists clear classification within the space of international legal geography.

The IETF is not the only entity that exerts this type of multistakeholder control. Both the Internet Society (ISOC) and the W3C (see Chapter 3) as Internet governance communities share attributes with the IETF, though the IETF is the most extreme in its extra-stateness. While these are both interesting cases, the warping of international legal geography is observed better in a case with different attributes. Such a case can be found in the Internet Corporation for Assigned Names and Numbers (ICANN), which currently exists as a non-profit corporation under the laws of the U.S.

ICANN was also a product of the ad hoc historical processes through which computer scientists pieced together Internet governance. In the 1970s, Jon Postel began the work that would later be known as the Internet Assigned Names and Numbers Authority (IANA). Postel's work would eventually develop into a regime for managing the DNS, described above in Chapter 2. At this point in time, the Internet was largely made up of U.S. government and University networks. The U.S. National Science Foundation (NSF) was the lead government agency, and it left governance of Internet architecture up to the coders and engineers that were making the technical decisions on how to best foster interoperability on the network. Postel emerged as a one-man show at the University of Southern California, and he managed the root file of the DNS through an NSF contract.[43] The U.S. government's policy during the 1990s was to leave the development of the Internet to "private sector leadership" in hopes of privatizing the network of networks.[44] The U.S. federal government, though, soon stepped in as a reaction to various proposals for privatization of the IANA function that began to arise in 1994.[45] This action resulted in ICANN "[a]s an alternative to government."[46] ICANN was created by Postel to take over the IANA function, and it signed its first Memorandum of Understanding with the U.S. Department of Commerce in November of 1998.[47] ICANN is "a private nonprofit corporation created to manage policy and technical features" of the DNS.[48] The corporation itself functioned with oversight by the National Telecommunications and Information Administration (NTIA),[49] which maintained a "back door authority"[50] that it used to "very rarely reject" ICANN action.[51] This oversight does play an "important role in ensuring that proper processes are followed."[52]

Three things of significance should be noted here. First, ICANN has personality under U.S. law making it subject to the law of the United States. Second, despite the fact that ICANN extends from U.S. government involvement in the development of the Internet, there was never any sort of lawmaking procedure, other than a contract, that gave ICANN its authority.[53] It administers a significant governance regime that developed outside the realm of lawmaking in the domestic and international arenas.[54] Third, despite this extra legality, ICANN is subject to special government intervention through NTIA oversight function.[55] Thus on its face, ICANN fits into the state's governance structure and seems dissimilar from organizations like the IETF.

However, in 2014, the NTIA "unexpectedly" announced its intention to transfer the IANA functions of ICANN to a multistakeholder regime.[56] This serves an interesting example of a state relinquishing control of an Internet governance body, but the relinquishment is not to the international community as might be expected. The announcement stated that the NTIA would "transition key Internet domain name functions to the global multistakeholder community."[57] Notably, the announcement employs the word 'global' as opposed to 'international.' In fact, the word 'international' only appears one time in the announcement compared to 'global's' six.[58] This indicates an intent to not turn IANA over to an international organization. Instead, the announcement posits a new form of governance body, a global multistakeholder community, that is undefined in international law. The NTIA announcement came shortly before the NETmundial conference held in Brazil in April of 2014. This civil society conference adopted a Statement on Multistakeholder Governance, which helps to shed light on the idea of a "global multistakeholder community." It states that:

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 users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the issue under discussion.[59]

An obvious implication in this statement is that the state is just one of numerous stakeholders, and the NTIA announcement proximity to this highly publicized meeting indicates a conscious decision of the NTIA in choosing the term 'multistakeholder.'

The NTIA contract with ICANN ended on 1 October 2016. The technical and operational aspects of IANA was transferred to Public Technical Identifiers (PTI), which is an affiliate of ICANN. Though the transition can be seen as a reaction to controversies over ICANN's "legitimacy and ties to the U.S. Government,"[60] the contract between ICANN and PTI requires that PTI be located in the U.S., giving the U.S. some amount of leverage over the operational mission of PTI.[61] Despite this PTI maintains that it "aim[s] to not directly set policy by which [it] operate[s]."[62] That policy comes from ICANN supported forums meaning that "policy development for domain name operations and IP addressing is arrived at by many different stakeholders."[63] In multistakeholder governance states are just "one type of stakeholder," which removes them from their usual place of dominance in world-scale governance.[64] The state as a result is functioning in a new legal geography which differs from that of international governance.

The IANA functions administered by ICANN are a "global regulatory regime."[65] The numbers they control are referred to as "critical internet resources," and these numbers define what devices are on the Internet and, thus, who is in Cyberspace.[66] ICANN also manages domain name dispute resolution administering a nonjudicial arbitration system, the Uniform Dispute Resolution Policy (UDRP), through which intellectual property disputes can be resolved.[67] ICANN manages these property rights in Cyberspace, specifically, because the state has limited ability to do so. Interoperability on the Internet necessitates a uniform root file. If two states were to resolve a domain name dispute differently, this could result in either an inability of one of these states to enforce its judgement or a fragmenting of the root file and thus the Internet. At the moment, parties can pursue a domain name disputes in U.S. Federal Court, because it has jurisdiction over ICANN and PTI. This same jurisdictional authority allows U.S. law enforcement to seize domains associated with criminal activities.[68] The power of the state is still a real one, but the U.S. lacks the ability to consent on how the DNS regime and its regulatory aspects develop.

States are just one voice in multistakeholder governance, and their consent to be bound is not a necessary precursor for the adoption of a rule.[69] These Internet governance communities change the dynamic of a state's authority over transnational communications, and this is a new development in world-scale government. IGCs are not the only entities changing authority. Private corporations are also taking a seat at the multistakeholder table, and they perform a number of governance functions in Cyberspace.

Corporate Governance

As addressed in the first section of this chapter, states have traditionally maintained control over information at their borders. Their ability and right to control information at their borders was based on their ability and right to control information within their borders, a right that flowed from sovereignty as recognized in the international system. This is why states may have laws that set the extent to which citizen speech is protected, as well as why states have legal controls over intellectual property. In this system, citizens rely on the state to protect their speech rights and companies must rely on states to protect their intellectual property.[70] But digitization has changed the nature of both speech and property, making both difficult for the state to regulate effectively by exponentially multiplying the sites where such interactions occur.

Digitization makes information super-portable. Media of all sorts can be digitized and sent across the Internet. This means that a song, for instance, can be encoded as an MP3, attached to an email, and sent to a friend. This is the basic concept for one of the early business ventures on the Internet: Napster. Napster allowed individuals to share files with other users of the program by enabling peer-to-peer connections. This proved to be wildly popular with college students using high bandwidth connections to share music. While this was a great boon for individuals looking for digital files of their favorite songs, record companies were predictably concerned with such technologies, because the technologies enabled the copying and distribution of their copyrighted intellectual property.

As the Napster case foretold, intellectual property would become, and still is, one of the most heated battlegrounds in

Internet law and policy. Though Napster's business model was stopped by the US legal system, a number of services filled its space with different technical specifications meant to subvert the law that was used to shut down Napster.[71] Copyright is not the only area of intellectual property that has been affected by Cyberspace, though it may be the most prominent. Trademark, as noted above, has been one of the biggest issues in ICANN's management of the DNS,[72] and patent has been implicated as corporations have attempted to protect the code that they use in Cyberspace.[73]

The reason that intellectual property has become such a contentious issue in Cyberspace is twofold. First, digitization makes sharing of intellectual property easy. Intellectual property can be perfectly copied and transmitted across the Internet with ease.[74] The MP3 files that made Napster a phenomenon, could be easily copied without generational degradation associated with analog media. This means that digital files, such as a copyrighted song, can be perfectly copied and shared on massive scales when users are able to connect using peer-to-peer using technologies such as BitTorrent.[75] The means of efficient copying have been combined with the means of efficient distribution.

The second issue fueling this debate is linked to the competing business models in Cyberspace. In analog media space, while there is a black market for intellectual property, content owners are generally responsible for the production and distribution of their property. Record companies, for instance, copy the songs they own onto CDs and sell them at record stores. They control the physical copying and distribution in such a way that it diminishes the ability of others to copy and share that information. In a digital environment, intellectual property holders have the same goals: to make a profit from the sale or use of their intellectual property, but the structure of the environment in which they pursue these goals is dramatically different in Cyberspace. Users no longer enter record stores to buy music; they enter search terms. The results of that search might send them to the record company or a licensed distributor to buy the music, but it is just as likely to send the user to a third party that is distributing free copies of the file. Cyberspace creates a gap in interests between the content owner and the content distributor, the Internet Content Provider (ICP).

To see this gap in action, one merely needs to visit YouTube, an online video sharing website owned by Google.[76] YouTube's business model is based on user generated videos spawning web traffic to the site, which nets YouTube profits through revenues from ads served to users that visit the site. In basic terms, YouTube's business interest is in having as much content as possible available through its servers. More content brings in more viewers. An ICP's business goals are often in direct conflict with intellectual property owners that want to control the dissemination of their content. This has created a clash between content owners and ICPs that has played out across a number of fora and has been the subject of domestic lawmaking, but an important trend can be traced as these intellectual property disputes have proliferated. There has been a ceding of power to commercial entities who control the content available in Cyberspace. This power is often exerted without recourse to formal legal procedures contained within the legal geography of the state.

In the case of intellectual property, this can be seen in the notice and take down procedures deployed in numerous states to balance the competing interests of content owners and ICPs who host user uploaded content. Under these regimes, content owners must give notice to the ICP that it is hosting protected content on its website. In return, the ICP is granted a 'safe harbor' from legal liability by promptly taking down the content. The user is then given notice that the content has been removed. In the US context this is often referred to as being 'DCMAed,' a reference to the U.S. Digital Millennium Copyright Act (DMCA), the law that enacted the US regime for notice and takedown.[77] While the equities between the content owner and the ICP seem fair here, many scholars have noted that these regimes result in a burden being shifted to the user. So, for instance, going back to YouTube, if Warner Bros.'s identifies a clip from one of its films, then it fills out an online form which notifies YouTube. The clip is removed, and the user is sent an email notification informing them of the takedown. The user is then given the option to send a counter notification if they think the takedown has been in error. The information page on the counter notification process informs the user that his or her personal information will be revealed and that the "claimant may use this information to file a lawsuit against you."[78] Users are left with the decision of whether they want to pursue a claim in which they are most likely out-gunned. This burden shift means that corporations can over protect their content and block potentially valid uses such as parody or fair use based on the odds stacked against the user.[79]

Notice and takedown turns corporations and the technology they deploy into mediators of speech. Such mediation also takes place in the realm of self-regulation where corporations agree amongst themselves on how to best conduct their business. Self-regulation in the sphere of content standards in the domestic context has been a feature of broadcast telecommunications that has been widely adopted in the context of Cyberspace.[80] Self-regulation of content within an interoperable arena is vastly different from broadcast and raises novel questions as to the extent that private companies should be able to control speech online. As DeNardis and Hackl note, private actors are increasingly implementing technical architectures that mediate what speech is acceptable and what speech is not.[81]

In the context of particular social media sites this seems to be just the sort of community governance contemplated by early netficianados such as Barlow. It also reveals a startling removal of the state from the regulation of the political space in which speech takes place. It shifts power away from the individual by removing the court from between the individual and those that would suppress expression. In the place of the court are corporations that are seeking to maximize profits, rather than protect user rights. Laws like the DMCA, incentivize both intellectual property owners and ICPs to over protect data. This means that on the Internet "the rules of copyright law, as interpreted by the copyright owner, get built into the technology that delivers copyright content."[82] As a result, Cyberspace has "revealed the nexus between copyright and communications law, and the impact of both on speech."[83]

While mechanisms such as user agreements are a natural way to govern speech within the "walled gardens" of user experiences, the debate over net neutrality reveals a more troubling implication of corporate governance. Net neutrality, discussed in Chapter 2, centers on whether an ISP may legally favor some data or disfavor other data.[84] So, for instance, an ISP could enter a contractual agreement with a video streaming service for its data to move faster or to block data from a competitor's server or to slow certain types of data. ISPs say that they need this capability to efficiently manage their bandwidth, but those in opposition claim that if net neutrality erodes then ISPs will effectively control the content that users receive.[85] This means that "[e]ven routine technologies of bandwidth management are value-laden."[86] Media companies now must fight for the attention of viewers amidst a din of competition, and these same media companies have converged along with the technologies on which they operate, meaning that intellectual property owners are often ISPs as well. For instance, two of the largest broadband providers in the United States, Comcast and Time Warner, also function as ICPs and intellectual property owners.

From these examples, a few key features of corporate governance can be observed. First, there is a severe lack of transparency when a corporate actor takes action against speech on the Internet, as there are no accepted procedures for such action. Second, this puts a severe burden on the individual to enforce his or her speech rights as there is a large imbalance of power between the corporate entity and the individual. Third, individuals may not even know whether their speech or access to information has been limited due to the nature of technical architecture. Finally, and most importantly, the state is passing these powers to the corporations involved to enforce directly. Notice and takedown is a statutory process, but it is one that removes the state as the central mediator of rights making it a peripheral entity in the process.

Other such mechanisms exist as well. The Copyright Alert System is the result of an agreement between ISPs and major copyright holders in which ISPs agree to use a tiered system to discourage copyright violators.[87] Under the agreement repeat violators can have their access to the Internet through the ISP eliminated.[88] Another example is the European 'right to be forgotten' which allows individuals to demand content about themselves to be removed from ICPs.[89] The right to be forgotten also suffers from the burden shifting that occurs with notice and takedown schemes for intellectual property.[90] Similarly, Maurushat and Shachtman both argue that ISPs are in the best position to regulate cybercrime.[91] These examples all point to a trend in which "the determination of conditions of participation in the public sphere is increasingly privatized."[92]

The governance mechanisms "delegated" to "private intermediaries" are not just economic in their effects.[93] For example, Tambini et al. note that self-governance by corporations implicates them as the mediator of the right to expression.[94] Relatedly, Sunstein notes the effects of how commercial forums can be tailored into echo chambers that restrict deliberative democracy.[95] Finally, Lessig implicates corporate governance of intellectual property with the production of culture itself.[96] This means that corporations now "play a key role in ensuring and enabling" a number of human rights, especially "when an operator is dominant."[97] As a result, a Council of Europe report

argues that Internet governance should be maintained in a way that "avoids predominance of particular deep-pocketed organizations that function as gatekeepers for online content."[98]

This is not to say that governance by corporations is a particularly new innovation. Many European empires of the 18–19th centuries were essentially corporations licensed to go out and govern, and neoliberal processes are premised upon MNCs effectively wielding power.[99] In fact, the rise of the Internet as a global force can be traced to a U.S. preference for "private, and avowedly economically rational, mechanisms of self-regulation."[100] There is, however, something distinctive about this in the context of Cyberspace, since "[f]unctionalist and technologist concerns regarding security, encryption, and domain name allocation become increasingly difficult to separate from the individual rights concerns regarding privacy, freedom of expression and public governance of the commons."[101] MNCs in this context are mediating the rights of individuals regardless of their location. A platform like Twitter, which is often mentioned in the same sentence with phrases like "global public sphere," can implement regulations that are effective globally and without any sort of public debate over these regulatory changes. In Cyberspace code is law, and this means that those who control code have authority. While states have the ability to regulate the code that will be implemented in their borders, for instance China's Great Firewall, corporations still maintain large areas of authority over users traversing their networks, and that authority often extends non-concurrently with the jurisdictional borders of the state from which the corporation is working from.

—

The international governance system is designed to allocate authority in a particular legal geography, in which the sovereign territorial state is the core political unit from which authority is to flow. This authority flows in two directions: it makes the state the sole holder of authority within the bounds of its territory, and it makes the states the holders of authority to take part in international governance processes. This is why the international community has had such a difficult time dealing with mass atrocities. In order for the international community to stop such atrocities happening within the borders of a state, it must undermine its own spatial ordering.

Cyberspace presents a different legal geography that saps authority away from the state as a holder of international rights. Authority in this new legal geography is vested in those that control the development, the adoption, and the deployment of code that operates at a global level. The ITU's regime for governing telecommunications is focused on physical phenomena that clearly occur at borders. Cyber-technologies, in particular the logical layer of the Internet, are ubiquitous, and regulation tied to the physical and legal geography of borders has proved to be ill suited for governing these technologies. Cyberspace wields its own authority, which is embedded deep within the code that architects its geography. The next and final chapter in this section will explore how this change in authority affects the rights of the individual engaging in the public sphere of Cyberspace. It will specifically engage with how changed territoriality and changed authority have reallocated the relationship between the individual and the state by introducing new ways of mediating rights.

Notes

[1] *See* Battaglia, "Arresting Hospitality" (2012) S76–S89.

[2] *Id.* at S82. *See also* International Docking System Standard, Interface Definition Document, Revision D (2015).

[3] *See generally* Charlotte Hooper, *Manly States* (2001).

[4] S*ee generally* Jayakar, "Globalization and the Legitimacy" (1998) 721–722.

[5] Codding, "The International Telecommunications Union" (1994) 501.

[6] *Constitution of the International Telecommunication Union* (2010) preamble.

[7] Eppenstein & Aisenberg, "Radio Propaganda" (1979) 154.

[8] *See* Lyall & Larsen, *Space Law* (2009) 256–269 and UNGA, Res. 37/92 (1982).

[9] *Constitution of the International Telecommunication Union* (2010) Art. 1.2(b), Art. 45 and Eppenstein & Aisenberg, "Radio Propaganda" (1979) 154.

[10] Codding, "The International Telecommunications Union" (1994) 505.

[11] *See Constitution of the International Telecommunication Union* (2010) Art. 21.

[12] Held, *Democracy and the Global Order* (1995) 109.

[13] *Constitution of the International Telecommunication Union* (2010) Art. 2

[14] Jayakar, "Globalization and the Legitimacy" (1998) 717.

[15] *Id.* at 728–729. DeNardis, *The Global War for Internet Governance* (2014) 33.

[16] Finnemore & Sikkink, "International Norm Dynamics and Political Change" (1998) 893.

[17] *Radio Regulations* (2012) Art. 1.3

[18] Jayakar, "Globalization and the Legitimacy" (1998) 719.

[19] DeNardis, *The Global War for Internet Governance* (2014) 33.

[20] Dickinson, "How Will Internet Governance Change after the ITU Conference?" (2014).

[21] United States Department of State, "Outcomes from the International Telecommunication Union 2014 Plenipotentiary Conference" (2014).

[22] *Id. See also* Dickinson, "How Will Internet Governance Change after the ITU Conference?" (2014).

[23] United States Department of State, "Outcomes" (2014).

[24] *See also* ITU, "Resolution 133 (Rev. Busan, 2014) Role of Administrations of Member States in the Management of Internationalized (Multilingual Domain Names"; ITU, "Resolution 140 (Rev. Busan, 2014) ITU's Role in Implementing the Outcomes of the World Summit on the Information Society and in the Overall Review by United Nations General Assembly of Their Implementation"; and ITU, "Resolution 180 (Rev. Busan, 2014) Facilitating the Transition from IPv4 to IPv6."

[25] ITU, "Resolution 2 (Rev. Busan, 2014) World Telecommunication/Information and Communication Technology Policy Forum."

[26] ITU, "Resolution 101 (Rev. Busan, 2014) Internet Protocol-Based Networks."

[27] ITU, "Resolution 102 (Rev. Busan, 2014) ITU's Role with Regard to International Public Policy Issues Pertaining to the Internet and the Management of Internet Resources, Including Domain Names and Addresses."

[28] IETF, "Tao of the IETF" (2012).

[29] Johnson & Post, "Law and Borders" (1996) 1375.

[30] *Id.*.

[31] Walzer, "The Moral Standing of States" (1980) 211 and Clark, *Legitimacy and International Society* (2005) 6.

[32] Power & Tobin, "Soft Law for the Internet" (2011) 41.

[33] Alvestrand & Lie, "Development of Core Internet Standards" (2009) 126 and DeNardis, *The Global War for Internet Governance* (2014) 36.

[34] DeNardis, *The Global War for Internet Governance* (2014) 65–66.

[35] Halvorssen & Lloyd, "We Hacked North Korea With Balloons and USB Drives" (2014).

[36] *See* Leiner *et al*., "A Brief History of the Internet" (2012) and Power & Tobin, "Soft Law for the Internet" (2011) 41.

[37] IETF, "Tao of the IETF" (2012).

[38] Jayakar, "Globalization and the Legitimacy" (1998) 736.

[39] DeNardis, *The Global War for Internet Governance* (2014) 77.

[40] Alvestrand & Lie, "Development of Core Internet Standards" (2009) 126.

[41] DeNardis, *The Global War for Internet Governance* (2014) 69.

[42] Alvestrand & Lie, "Development of Core Internet Standards" (2009) 126.

[43] Mueller & Thompson, "ICANN and INTELSAT" (2004) 66–67.

[44] *Id.* at 63.

[45] *Id.* at 67–68.

[46] *Id.* at 63.

[47] *Id.* at 68.

[48] Rosenzweig *et al*., "Protecting Internet Freedom and American Interests" (2014) 1; Zalnieriute & Schneider, "ICANN's Procedures and Policies in the Light of Human Rights, Fundamental Freedoms and Democratic Values" (2014) 9; Partridge & Lonardo, "ICANN Can or Can It?" (2009) 24; and DeNardis, *The Global War for Internet Governance* (2014) 48–49.

[49] *See generally* Krattenmaker, *Telecommunications Law and Policy* (1998) 21.

[50] Mueller & Thompson, "ICANN and INTELSAT" (2004) 70.

[51] Rosenzweig *et al*., "Protecting Internet Freedom and American Interests" (2014) 3.

[52] *Id.*

[53] Mueller & Thompson, "ICANN and INTELSAT" (2004) 65, 69.

[54] Mueller & Thompson, "ICANN and INTELSAT" (2004) 63 and DeNardis, *The Global War for Internet Governance* (2014) 46. *But see* Rosenzweig *et al*., "Protecting Internet Freedom and American Interests" (2014) 4.

[55] Partridge & Lonardo, “ICANN Can or Can It?” (2009) 24.

[56] Rosenzweig *et al*., “Protecting Internet Freedom and American Interests” (2014) 1–2.

[57] NTIA, “NTIA Announces Intent to Transition Key Internet Domain Name Functions” (2014).

[58] *Id.*

[59] NETmundial, NETmundial Multistakeholder Statement (2014).

[60] Partridge & Lonardo, “ICANN Can or Can It?” (2009) 24 and DeNardis, *The Global War for Internet Governance* (2014) 61–62.

[61] ICANN-PTI, IANA Naming Function Contract (2016) Sec. 4.2

[62] IANA.org, “About Us” (n.d.).

[63] *Id.*

[64] Hurwitz, “A New Normal?” (2013) 239.

[65] Mueller & Thompson, “ICANN and INTELSAT” (2004) 77.

[66] Denardis, *The Global War for Internet Governance* (2014) 57–58 and Mueller & Thompson, “ICANN and INTELSAT” (2004) 77.

[67] Partridge & Lonardo, “ICANN Can or Can It?” (2009) 24–29.

[68] DeNardis, *The Global War for Internet Governance* (2014) 184–189; Gallagher, “Silk Road, Other Tor ‘darknet’ Sites May Have Been ‘decloaked’ through DDoS [Updated]” (2014); and Mueller & Thompson, “ICANN and INTELSAT” (2004) 81.

[69] Leiner *et al*., “A Brief History of the Internet” (2012).

[70] *For example* US Constitution, Art. 1.8.8, 1st Amend.

[71] Lessig, *Free Culture* (2004) 73–74.

[72] *See generally* Partridge & Lonardo, “ICANN Can or Can It?” (2009).

[73] *See generally* Vera Ranieri, “EFFecting Digital Freedom” (2014–2015).

[74] Lessig, *Free Culture* (2004) 62–79.

[75] DeNardis, *Global War for Internet Governance* (2014) 63–65.

[76] http://www.youtube.com

[77] Digital Millennium Copyright Act, Pub. L. 105–304 (1998). *See also* Lessig, *Free Culture* (2004) 157.

[78] YouTube, “Copyright Counter Notification Basics” (2019).

[79] *See* Goodman, “Media Policy and Free Speech” (2007) 1233.

[80] *See generally* Tambini *et al*., *Codifying Cyberspace* (2008).

[81] DeNardis & Hackl, "Internet Governance by Social Media Platforms" (2015).

[82] Lawrence Lessig, *Free Culture* (2004) 148.

[83] Goodman, "Media Policy and Free Speech" (2007) 1212.

[84] DeNardis, *The Global War for Internet Governance* (2014) 131–32.

[85] Verizon v. FCC (2014) 6.

[86] DeNardis, *The Global War for Internet Governance* (2014) 8.

[87] Center for Copyright Information, "FAQ's on The Center for Copyright Information And Copyright Alert System" (2011) and Kravets, "ISPs to Disrupt Internet Access of Copyright Scofflaws" (2011).

[88] *Id.*

[89] *See generally* Rosen, "The Right to Be Forgotten" (2012) 88.

[90] *Id.* at 91–92.

[91] Maurashat, "Zombie Botnets" (2010) 379 and Shachtman, "Pirates of the ISPs" (2011).

[92] DeNardis & Hackl, "Internet Governance by Social Media Platforms" (2015) 6.

[93] DeNardis, *The Global War for Internet Governance* (2014) 13.

[94] Tambini *et al*., *Codifying Cyberspace* (2009) 275. *See also* DeNardis, *The Global War for Internet Governance* (2014) 157.

[95] Sunstein, *Republic.com 2.0* (2007).

[96] Lessig, *Free Culture* (2004) 28–30. *See generally* Serageldin, "Cultural Heritage as a Public Good" (1999) 240–63.

[97] Council of the EU, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (2014) I.D.34.

[98] Zalnieriute & Schneider, "ICANN's Procedures and Policies in the Light of Human Rights" (2014) 16.

[99] *See generally* Burbank & Cooper, *Empires* (2010) 149–184.

[100]Tambini *et al*., *Codifying Cyberspace* (2009) 15.

[101] *Id.*

About the author:

P.J. Blount is a Post-doctoral researcher at the University of Luxembourg in the Faculty of Law, Economics, and

Finance. His research focuses on space and communications law. Previously he served as a Research Counsel and Instructor at the University of Mississippi School of Law; was a Visiting Scholar at the Beijing Institute of Technology, School of Law; and an Adjunct Professor at Montclair State University, Department of Political Science and Law.