This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Reprogramming the World: Legal Terrains

https://www.e-ir.info/2019/12/06/reprogramming-the-world-legal-terrains/

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.

One of the most striking things about air travel is the labyrinthine airport layouts that create and demarcate a variety of distinct spaces for the traveler. Passengers move through underground passageways and shopping mall-esque avenues en route to boarding their airplane. They move from a non-sterile zone to a sterile zone after crossing security borders that demarcate changes in rules. While travelers experience these layouts as minor annoyances, they often fail to recognize how airports are architected to control the travelers within them. Airports by design demarcate and produce the rules of behavior within different zones of space. This is not a characteristic unique to airports, as nearly all architecture deploys some sort of control.[1] For instance, architected control is the underlying premise of Jeremy Bentham's Panopticon, but it can be also seen deployed in the layouts of public spaces such as Walmart stores and museums.[2] Architected control is visible in private spaces as well, as doors and walls are architectural mechanisms that help to maintain privacy. Architecture controls how individuals experience space by enabling and disabling them in a variety of ways, and Cyberspace's open network architecture is no different. Along these same lines, airports use architecture to segregate international passengers, particularly international arrivals, from the rest of the airport population. International passengers are ushered into arrivals halls that are designed with a series of counters at which sits an authority of the state that checks the passport and documentation of each traveler. There are signs that indicate that this line of counters is the border of the country at which the plane has landed. Despite the fact that these travelers are usually deep within the interior of the territory of that state, they have not yet entered the state. In this case, the geography of the border is warped to match the legal geography of jurisdiction, creating nearly unmappable zones of exclusion on a map of national borders.

These examples illustrate different sides of the same coin. Legal geographies can be deployed by technologies of enforcement to limit individual ability to transgress the norm being enforced. Additionally, these geographies can also be reimagined to include or exclude space despite the physical location of that territory. The state's ability to dynamically conceptualize its borders in such a way as to create legal fictions within territory renders borders into markers of a legal geography based on jurisdiction.[3] This is why architectures of control are used at borders: they give materiality to imaginary lines, because state's borders are only as solid as the state itself can make them. The legal geography of Cyberspace is a question of how architectures of control are deployed within it. The analysis here applies across the layered model established in Chapter 2. First, it will probe the idea of jurisdiction as a type of geography. To do this it will examine the traditional link between territory and jurisdiction. The second section will use the link between architecture and control to examine a fundamental principle of how regulatory power is distributed in Cyberspace through examination of Lessig's principle that "code is law." Finally, this chapter will turn to the idea of code as a constitution of Cyberspace and explore the governance implications that flow from such an idea. This final section will then draw conclusions on the dispersion of jurisdiction in Cyberspace.

The Space of Law

Jurisdiction is the space of law. It can be understood, in at least one sense, as the literal geographic limitations of the law.[4] As a legal concept, jurisdiction can seem ephemeral, but it is literally part of the language that we use to locate ourselves within the world. "I'm from …" is a phrase that is likely to end with a designation of a legal jurisdiction such

as a state or its political subdivisions such as provinces, counties, or municipalities. These subdivisions, which are often nested like matryoshka dolls, each denote space with a particular set of legal characteristics. This is what is meant by legal geography. Importantly, these nested jurisdictions overlap in such a way that an individual is often standing in a hierarchical stack of overlapping jurisdictions. It is argued herein that Cyberspace also deploys a legal geography of jurisdiction over the individual, but this geography resists containment within jurisdictions as conceptualized in the international governance regime.

As noted in Chapter 2, Cyberspace alters our spatial experience. Jurisdiction, in the modern state system, is linked directly to territory. Territory serves as the critical link between jurisdiction and power in a state's deployment of governance, because historically there has been "a general correspondence between borders drawn in physical space … and borders drawn in 'law space.'"[5] This is by no means a 'natural' connection, but it has been a de facto connection based on technologies through which power is exerted and through which global order unfolds.

To this end, international law has recognized five bases from which a state may extend its jurisdiction and thereby exert its power: territorial, personal, protective, passive personality, and universal.[6] Each of these principles for extending jurisdiction has their own internal logic, but all – save one – are tied back to physical territory. This embeds territorial understandings into the concept of jurisdiction within international space.[7] Personal jurisdiction is linked back to a territory via auspices of nationality; protective jurisdiction is linked to protecting the territory of the state from harm; and passive personality links to the concept of nationality, which in turn links to territory. Only universal jurisdiction seems to evade the territorial link, because its original incarnation was as a mechanism to address actors external to the territorial borders of any state, such as pirates.[8] Universal jurisdiction, though, does require that malefactors be brought into the territorial jurisdiction of the state in order for it to exert legal power.[9]

What these accepted principles of jurisdiction exhibit is that territory is foundational to jurisdiction in the international system, and that jurisdiction can be understood as the space in which the state can exert its power, both juridical power and through its monopoly on violence.[10] It is important to understand the territorial limitation of state power, because territory sits at the heart of the international legal system. The borders drawn by that system show a particular configuration of jurisdiction superimposed on the space of the world. While "[w]e take for granted a world in which geographical borders … are of primary importance in determining legal rights and responsibilities," this configuration is only a static rendering of a dynamic set of lines that indicate a variety of fluid spaces.[11]

The argument advanced by this section is that jurisdiction, understood as a legal geography, is neither a continuous nor a static space, and that it is reconfigurable not only through a state's own conceptualization of its borders, but also through external processes that reshape the nature of legal space. This section will proceed in two parts, both of which are designed to show the gaps in the link between territorial space and regulatory space. First, this section will show how Cyberspace fractures national jurisdiction, and then, it will pursue the same goal in terms of international space. It should be noted that the claim made in this section is not that state jurisdictions have wilted away, but that jurisdiction is not "already, and forever, 'settled.'"[12] The state retains a great deal of power in relation to objects and individuals within its territory. However, Cyberspace creates a spatial situation in which regulatory power associated with territory runs out, and at this point we can see where Cyberspace's legal geography begins.

National Space

The debate on the nature of Cyberspace, typified by the exchange between Post and Goldsmith discussed in Chapter 2, is important in the discussion of legal geography. The debate was centered on whether or not Cyberspace was a new space, but specifically as legal scholars, the dispute centered on whether Cyberspace created new alternative legal geographies of jurisdiction. Such claims had been advanced in Barlow's "Declaration of Independence for Cyberspace." Barlow's claim that states "were not welcome" in Cyberspace, is rooted in the notion of an independent territorial sovereignty as the source of legitimate governance in Cyberspace.[13]

While Goldsmith rejects such rhetoric outright, Post takes a more nuanced position. He claims that "cyberspace is somehow different" and that this difference "matters for the purposes of understanding these jurisdictional questions."[14] Post's argument is rooted in the idea that Cyberspace creates a world "of inter-connected and

geographically complex cause and effects."[15] He notes that

transactions in cyberspace can take place at much greater physical remove; they are consummated by means of the movement of bits rather than atoms; they are digitally encoded; they are unaffected by the participants' sense of smell; they are embedded in and mediated by computer software; they travel at the speed of light, etc.[16]

Massively distributed computer mediation of transactions, in Post's view, requires reevaluation of "settled understandings" of concepts such as jurisdiction.[17]

To understand Post's arguments, the critical gaze must again turn to the borders that define the state. Older transborder technology was often controlled by technological standards that were adopted by a given state. This was a unique function of legal jurisdiction that could create architectural controls at the border of a state. For example, by adopting a different standard railroad gauge a state could ensure that all train shipments were disembarked and reloaded under the state's watchful eye.[18] Standard setting is a tool by which technology is directly regulated. The logical layer of the Internet adopts standards that enforce universal interoperability, meaning that the logical layer bypasses borders by rendering a state's physical telecommunications standards irrelevant. The physical technology of the border is undermined as Cyberspace reroutes border crossings to the applications layers running of the Internet. The proliferation of transaction points also drives the proliferation of border intersections. For the territorial border, "[d]igitization means dematerialization."[19]

This is not to say that border crossing technologies have not been issues for the international community before. Indeed, radio transmissions[20] and satellite broadcasting[21] both caused debate in the international arena. As Post notes though, the scale of Cyberspace is dramatically different from previous technologies.[22] The ability to instantaneously communicate with the entire online population forces new understandings of jurisdiction, since this means that data transmissions cross all borders at once.

The architecture of Cyberspace is such that it forces geographically remote states into direct contact with each other by bringing their borders together. This often means that "multiple noncoordinating jurisdictions" are brought into proximity as the Internet networks those jurisdictions into contact.[23] Cyberspace creates contact points between and among all networked physical space. This is problematic because laws "mostly concern national spaces."[24] This can be seen in the quintessential France v. Yahoo! case.[25] Suit was brought against Yahoo! in France because Yahoo! maintained an auction website that facilitated the sale of Nazi paraphernalia, which is illegal in France.[26] Yahoo!, an American company, was held culpable in France for the availability of this website within France's territory.[27] Two things should be made clear. First, this website was available to anyone with an Internet connection and a web browser regardless of location. Second, France's legal claim was only that the availability within the territory of France was illegal. If Yahoo! capitulated to the French demand for removal, the website would not be available anywhere in the world, including places where sale of such memorabilia is legal, leading to French law and values being enforced globally. Yahoo! sought a declaratory judgement in a United States federal court to render the decision unenforceable, but the 9th Circuit declined to grant the declaratory judgement on the grounds that it did not have jurisdiction over the French entity LICRA, which brought the original suit.[28]

While the cyber-unexceptionalist might argue that this is indicative of courts being perfectly capable of applying law to cases involving Cyberspace, the Yahoo! case has deeper implications that make such a stance tenuous. If this transaction were to occur in a pre-Internet environment there are a number of factors that would have made it different. First, a French citizen would need to leave France in order to take part in the auction making it a costly endeavor. That citizen would then need to physically transport the item over the French border and negotiate regulatory pressure points applied at border crossings. The Internet on the other hand allows all French citizens to take part in auctions that are "in" the United States in terms of server location. Three things are important here. First, the border crossing is not physical. This means that the state has lost some control over where its border is drawn. Second, the border crossing occurs on a private network. The state's apparatus for controlling borders is located physically at the borders in the form of checkpoints, which are places of inclusion and exclusion. In this case, the "checkpoint" has been routed around and the state has been excluded from its usual control function. Finally, the scale of Yahoo!'s actions are at a much different level of magnitude, as actions in Cyberspace have a "multi-site

effect" fragmenting the idea of *the lex loci*.[29]

Yahoo!'s auction site allowed everyone in France with Internet access to take part in these auctions by minimizing the transaction costs associated with borders. The physical geography pre-Internet stood as a barrier to all but the wealthiest and most dedicated of collectors. Now technology facilitates easy access by all to these auctions. Yahoo! was acting within the jurisdiction of France, yet France lacked the jurisdictional capacity to reach out and physically touch Yahoo! meaning that jurisdiction tapers as France's territory runs out. Before the Internet such interactions were marginal, but post-Internet they are facilitated.[30]

Jurisdiction as a function of territory requires that transactions be located "geographically somewhere in particular," which is "most unsatisfying."[31] The enduring lesson from Yahoo! is that state control over persons and property is being diminished as the borders that define that jurisdiction no longer represent a barrier to social transactions.[32] The space of the state runs out as a social space beyond its control opens.

International Space

Since the scale of transactions on the Internet is global in scope, many scholars have turned to international law as the way in which Cyberspace can be appropriately regulated. This approach is seemingly a natural one, since flows of information in Cyberspace are often transnational in nature, but this too presents several issues, and the dearth of international law addressing Cyberspace is telling.

First, it should be noted that the national is embedded in the international and vice versa. International space is a conceptual extension of national space.[33] The international system itself is made up of states that participate based on principles of nonintervention and sovereign equality.[34] As a result, modern international law is oriented toward the "territorial integrity" of the state itself.[35] International law reifies the geography of the state by rendering jurisdictional edges as borders of exclusion through the principle of nonintervention.[36] Indeed, until very recently, international law's regulatory focus was the border of the nation state, and only the most marginalized of territories are without legal standing in international law.[37]

States have long debated the control of transborder information flows as a matter of international law. Radio Free Europe and Voice of America are excellent examples of state attempts to penetrate the borders of other states with telecommunications technology.[38] But these interventions were limited in scope as both technology and geography ran out. Radio technology is limited by the ease of jamming as well as geographic constraints on the transmission power of the station.[39] Similarly, satellite technology raised issues resulting in a controversial set of principles adopted by the UN General Assembly.[40] Cyberspace is a new context for these same issues as it gives users "new opportunities for exchanging information and opinions."[41]

This concern with international communications is reflected in the international forum for addressing such issues, the International Telecommunication Union (ITU), which is the "oldest international organization in the world."[42] The ITU is the international organization (IO) tasked with coordinating international telecommunications with the "object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunications services.[43] The ITU has three sectors,[44] each with its own mandate: the Radiocommunication Sector "ensur[es] the rational, equitable, efficient, and economical use of the radio-frequency spectrum"[45]; the Telecommunications Standardization Sector which promotes standards that work across national borders[46]; and Telecommunication Development Sector which promotes the development of telecommunications systems in developing countries.[47] Cyberspace, while clearly a form of international telecommunication, does not fit distinctly within these well-defined silos of the ITU. As a result, the ITU has had little power to assert any sort of direct governance over Cyberspace.[48]

The gap that the ITU cannot fill has also been left empty by other international law-making processes. There is a notable dearth of treaty law. The only cyber-oriented, multilateral treaty is the Budapest Convention on Cybercrime, and it is weak at best.[49] The Budapest Convention attempts to set standards on the prevention and prosecution of cybercrime, but it falls short of being a document with any teeth to compel state action. Instead of strong

international obligations, the treaty shifts implementation and enforcement burdens to states and extends no jurisdiction by any international entity. By vesting right and obligation in the domestic system of the states, the Convention on Cybercrime reifies the central position of the state and ignores the vastly different governance dimension that Cyberspace presents. In fact, much of the scholarship on international law and Cyberspace seems to imply that it is an ineffective mechanism.[50] Sofaer et al suggest that cyber war, cyber intelligence, content restrictions, human rights, and national security will all remain outside the scope of international agreements.[51] Notably, conflict and human rights are specifically within the scope of extant international agreements, indicating a significant shift in power.

It is precisely the orientation to the national that has rendered international law ill-equipped to deal with the global nature of Cyberspace as it uses a siloed regulatory paradigm based on physical territory. While scholars have looked to both customary international law[52] and soft law principles,[53] there is little consensus on how cyber should be treated by nation states. The terrain seems to be frozen in terms of international law making.[54] This is not to say that states are unable to negotiate a treaty aimed at governing Cyberspace. They could do just that. The claim, instead, is that states are unable to deliver such a treaty, because they understand their own limitations in effectuating control in a sphere marked by severe jurisdictional uncertainty.[55] The non-territoriality of Cyberspace disembowels the notion of jurisdiction as contained in international law.[56]

A final distinction must be made. Chapter 2 posits a global location for Cyberspace, and it must be acknowledged that there are areas external to the state that exist within international space and are fully contemplated by international law. A group of areas known as global commons are defined within the bounds of international law, but outside the bounds of the national. The high seas, Antarctica, and outer space are all territories delineated by international law as global in nature.[57] Cyberspace does not fit within this category because it lacks a key common element with the global commons: Cyberspace is not a *res communis* in the sense contemplated by international law. [58] Global commons share a core legal prohibition against appropriation by a state. Cyberspace though, throughout the layered model, is marked by a dispersion of ownership with some components being owned by states themselves. Cyberspace emerged appropriated and is therefore not a global commons within the legal sense of the word, making it difficult to classify within the international system.[59]

Codes

The inability of national and international legal space to contain Cyberspace is rooted in the fact that users are "[s]eparated from doctrine tied to territorial borders."[60] In order to articulate a legal geography of Cyberspace, an inquiry into what regulatory mechanisms pick up when the territory of the state runs out must be made. Despite the fact that Cyberspace is sometimes compared to the Wild West[61] implying a degree of lawlessness, there are a number of sources of regulation in Cyberspace that exert control when and where the state cannot.[62]

As discussed in Chapter 2, Cyberspace has a technical architecture that sets its spatial boundaries and borders and serves to constrain inhabitants of that space. In the same way that a mountain range can prevent migration, the geography of Cyberspace is such that individuals can be stopped from migrating to certain networks as the result of virtual walls. The major difference – aside from one being virtual and the other existing in "meatspace" – is that Cyberspace is an architected geography.[63]

Cybergeography – i.e. its mountains and valleys and other "natural" attributes – is a manifestation of the code and hardware deployed across the layered conceptual model.[64] To conceptualize how code restricts, consider a simple example of the early arcade game *Pong*. Pong was a simple game that was released for the Atari game system in 1972.[65] In Pong, two players control blocks on the screen that function as paddles. These paddles are used to hit a dot on the screen, which represents a ball. The paddles that the players use move across a single axis, up and down, on the lateral ends of the screen, and the ball bounces off the top and bottom of the screen. Game play continues until one player misses the dot allowing it to pass the paddle and touch the left or right edge of the screen.

In other, less convoluted terms, Pong is an electronic version of ping-pong or table tennis. There is a critical difference, for the purposes at hand, beyond just the equipment needed for each version: in ping-pong a player can

break the rules. It is a game with a set of rules. Those rules constrain the players through threat of penalty, but there is possibility that the players can subvert and violate those rules.[66] In Pong, on the other hand, players are incapable of cheating. Pong's rules are enforced perfectly in the sense that players are compelled to obey them, not through threat of consequences for violation, but through compulsion of the game's architecture implemented through the computer code that sets constraints on the player within the game space. The rules are enforced perfectly, so players need not be given a rulebook or even notice of the rules to avoid violating them.

This example is used to illustrate Lessig's "code is law" principle.[67] Lessig's principle states that when technology of any sort mediates transactions, the code, or architecture, of that technology also regulates the possibilities for those transactions.[68] Regulation embedded into architecture can achieve near perfect enforcement because rules are compressed into the structure.[69] At the heart of Lessig's theory is the concept of regulability. He argues that individuals are "regulated" by a variety of forces including markets, law (in the formal sense), norms, and architecture or code.[70] Each of these forces exerts limitations on an individual's actions. Lessig posits that in Cyberspace "regulation is imposed primarily by code"[71]

Code regulates Cyberspace because it "defines the terms upon which cyberspace is offered."[72] The code is law principle requires analytic focus to be returned to the layered model wherein we can see the variety of architectures through which code is deployed. The layered model reveals specifically that there is code running across the bottom three layers that, combined, influence the user experience at the content level. These layers "are the unacknowledged legislators of cyberspace."[73] A benign example is Netflix, a website that streams movies to subscribing customers.[74] Netflix licenses distribution rights for intellectual property and makes that intellectual property available to view by its customers. Netflix has several core concerns in making its business model operate effectively and profitably. The first is avoiding theft in the sense of nonsubscribers gaining access to the Netflix collection. Netflix does not rely on a notice forbidding non-subscribers from entering the website under force of prosecution. This would plainly be futile. Instead, Netflix uses code at the applications layer that requires a subscriber to verify their identity in the form of a login using a username and password. Netflix discourages widespread sharing of these credentials by deploying code that limits the number of IP addresses (and therefore devices) that can access the collection from a single account at a given time. Second, Netflix is concerned with abiding by the terms of the distribution license it has with the owners of the intellectual property it streams. Netflix uses code at the applications layer to make movie files stream to user devices instead of fully downloading, which keeps Netflix from distributing unauthorized copies of the files.[75] License agreements are also likely to contain geographic restrictions on distribution. Netflix uses the user's IP address, which is part of the code of the logical layer, to filter out devices logging in from outside the territory in which the distribution license applies. Finally, Netflix wants its service to work for its subscribers. To do this it analyzes the bandwidth of the subscriber's connection and adjusts the resolution of the display accordingly to ensure smooth streaming. Bandwidth is highly dependent on the architecture of the physical layer through which the subscriber connects to Netflix. Netflix's user experience is shaped by the layered architecture. The user likely does not experience the code as regulations or rules that command compliance. Instead, all of the regulatory mechanisms – save IP filtering, which maps to territorial concerns – are likely experienced as functionality of the service.

Netflix is a benign example, but it highlights one of Lessig's key insights. Coded regulations are hidden in the architecture of the space. This means that regulatory effects are often experienced as functionality rather than limitation, meaning that hidden regulations can be developed and imposed outside of public scrutiny. Code hides from the user, and there is rarely conversation between the user and the developer as to how code is to function. Indeed, users may not have any notice at all of the rules or how they are being applied. In applications such as *Pong* and Netflix this can be of little importance to the user, but when considered in terms of a global network that interconnects individuals such hidden rules become problematic as machine mediated interactions proliferate. The code is law principle explains how the regulatory space is shaped, but opens the questions of the sources of code and how code is implemented.

Source Code: Software and Softlaw

Law comes from lawmakers. In a liberal democracy, it is, in theory, meant to be very easy to see from whence law

comes.[76] Transparency in law and regulation is a function of the liberal democratic system of governance. This system implements a standardized process for lawmaking, which creates openness in the public forums in which law is made and adjudicated. The standardized procedure allows for individuals to access the law. The coupling of transparency and procedure allows citizens to peer in and see how the laws that govern them are constructed and applied. This process hinges on legitimacy in the substance of the law being confirmed through the legitimating act of proper procedure. It also opens political space by setting a framework for government action.

Code comes from coders; that is, people who write code. Coders are everywhere. They can be employed by a government, contracted by a private entity, working as a collective for the public good, part of a criminal cartel, or working on their own for simple personal satisfaction. The motivations and goals of coders are non-uniform. They can be writing code for economic gain or public benefit. The code they release can be proprietary and secret, or it can be open and transparent. Code can be deployed at any of the layers of the layered model. The implication being that there is no standardized procedure for developing code and there is no open and transparent forum in which code as a category of regulation is debated. This is because in Cyberspace code is ubiquitous and non-monolithic.

Code, like the Internet itself, is rhizomatic in nature. It develops irregularly across space and time from multivariate, unpredictable sources, and it is deployed dynamically across networks that mediate interactions. This is a function of the end-to-end network, which has already been demonstrated to facilitate innovation at the edges of the network. Coders working at the applications layer to proliferate transaction points through the development of innovative applications. The open architecture literally allows an individual to change the legal geography of Cyberspace by writing code. For example, the Silk Road, an online marketplace for black market goods was programmed and operated primarily by a single individual.[77] The Silk Road changed the space of the online marketplace by facilitating anonymous transactions to remove the burden of state regulation.

Code must be understood as dispersed: across layers, across actors, across motivations. At any given time, a user in Cyberspace is being regulated by multiple layers of code. Operationalized, the 'code' is law principle means that it is difficult to discern applicable regulations when analyzing user level interactions. There is literally too much code for the user to evaluate, and the user must find ways to extend trust in code without needing to understand all code structuring interactions. Users can do this by using a variety of mechanisms such as user agreements, security certificates, trusted sources, etc. The practical result of this dispersion of code is that Cyberspace is embedded with a preference for self-regulation.[78] This result flows from the non-hierarchical architecture implemented in the logical layer.

States have significant power to oversee parts of this architecture, but not enough to regulate Cyberspace as a whole, because the decentralized nature of the network gives "all actors . . . an equally strong position in defining its nature."[79] It facilitates multiple entry points for co-regulators to deploy code. While states might use a device's IP address to reveal the identity of the individual using that device, Tor browser technology can be deployed at the applications level to encrypt and obscure a device's IP address thereby diminishing the reach of state's regulatory power and giving the individual the ability to choose rights inconsistent with those defined in the legal geography of the state.[80] Self-regulation allows for the dispersion of governance over a complex system, and it "is the laboratory of law and regulation for the Internet."[81]

The self-regulatory preference is salient because law has traditionally been an inefficient means of governing rapidly developing technology. Law moves slowly compared to technology, thus law can be slow to react to technological developments, and changes in technology can warp legal terms and entrench outmoded legal provisions.[82] This is one of the reasons that, in the modern bureaucratic state, lawmakers pass specificity down hierarchically to regulators, whose procedural rules make them more dexterous in rulemaking. These more dexterous means though are still burdened by formal procedure. Self-regulatory mechanisms perform a similar function, but are able to implement standards (i.e. regulatory mechanisms) by stripping process to a minimum and focusing on narrowly defined problems.

Cyberspace is big, and its architecture is designed to handle its massive scale.[83] One of the ways that it does this is by dispersing governance across public, private, and civil society networks and devices. As noted, the state holds

significant regulatory power over individuals and physical property, but Cyberspace governance is an assemblage, and the state is only one component of that assemblage. Similarly, international institutions such as the ITU and UN, despite their limitations, constitute another component of the assemblage as an expression of consensus, or lack thereof, of member states. The rest of the assemblage is composed of a variety of actors that work across the Internet's layers and exert different degrees of self-regulatory powers. For the purposes at hand, these non-state actors will be divided into three groups: commercial actors, civil society, and the individual. These groups are not discrete, and are chosen as representative points on a spectrum of actors.

Commercial Code

Commercial actors have long been considered to wield regulatory power, primarily through market forces. Indeed, Western European empires were built around private companies with the ability to extend regulatory authority through a lex mercatoria.[84] Commercial power is central to critiques of neoliberalism and the rise of the multinational corporation (MNC). One of the key lessons from globalization literature is the embeddedness of the MNC throughout the world, and its ability to skew law and policy through the extension of economic power has been confirmed.[85]

Cyberspace is, of course, no different. Commercial interests pervade three layers of the Internet. Corporations own physical infrastructure; corporations develop software at the applications layer; and corporations own content at the content layer. Only the logical layer is relatively free of direct corporate ownership and that is because the principle of interoperability requires the logical layer to be open, transparent, and the code free of proprietary claims. Corporations though are invested in the logical layer and are active in Internet Governance Communities (IGCs).

Tambini et al show that corporate self-regulation happens along industry divisions and is rooted in the notion "that conventional regulation involving legislative lag and inexpert courts, would be inappropriate and would risk breaking the architectural principles of this new technology."[86] Different industry divisions deploy self-regulatory mechanisms to ensure compatibility, user trust, and accountability. These groups use mechanisms such as codes of conduct, industry standards bodies, and interfaces that allow users to report norms violations in order to ensure compliance with the law as well as user satisfaction.[87] Self-regulatory activities by corporations are subject to the same critiques as self-regulatory bodies in other commercial areas. Questions of democratic deficits, the reification of power structures based on concentration of capital, and legitimacy are all raised for obvious reasons.[88] In Cyberspace, as Tambini et al observe, one of the central problems is that commercial bodies maintain control over information and how it flows, meaning that private interests become the arbiters of the "freedom of expression."[89] Importantly, corporations that exist in the global space of Cyberspace at a sufficient scale become the arbiter of this right across global spaces not linked to territorial jurisdictional limitations.

A second analytical problem caused by corporate self-regulation is that there are numerous different types of corporate actors. Phrases like "corporate interests" and "commercial interests" often indicate a unitary set of interests, but no such unitary interests can be identified for the 'Internet industry.' Self-regulation by commercial actors is architecturally dispersed and dependent on where a corporation functions within the layered model. Commercial actors innovating at the applications layer have an interest in maintaining open, end-to-end data transfers in the logical layer. This means that commercial interests owning physical infrastructure, like backbones and ICT networks are, due to market forces, required to maintain bandwidth sufficient to pass along the data required by the applications layer. The mismatch of interests, between content and bandwidth, can be seen in the net neutrality debate taking place in the US and Europe. The rise of streaming applications, such as Netflix, led to a steep rise in bandwidth requirements at the backbone level.[90] Due to the nature of agreements that arrange peering between backbones, the commercial owners were experiencing costs associated with increased bandwidth. The natural commercial solution to this problem is to pass those costs along to the entities using the bandwidth, and ISPs in turn want to pass those costs on to users. From a commercial perspective this is exactly how a market economy works, but this means that the ISP is also incentivized to give preference to some types of bandwidth usage.[91] As a result, an ISP and an Internet Content Provider (ICP) might enter into a contract that gives that ICP's content a priority to bandwidth or even excludes bandwidth traffic from a competitor. This could prove to be a viable profit stream to an ISP as well as potentially fatal to an ICP that lacks sufficient market power. ICP interest in providing

content implicates free expression issues as well as the innovative architecture of the Internet itself. If the end-to-end architecture fails to connect ends, then the space created by the technological landscape is dramatically changed. The point here is not necessarily to discuss the merits of net neutrality, but to show how corporate interests at different points in the stack of layers diverge. Net neutrality shows how a simple supply and demand issue at the physical layer permutates across the other Internet layers and reveals deep governance issues concerning the nature of the network and core human rights.

The net neutrality example reveals divergence of corporate interests, but it also reveals a convergence as well, namely that as technologies converge, corporations often merge. Many ICPs are not owners of the intellectual property rights in the content that they provide.[92] The control of intellectual property has been key contestation in Cyberspace and has a pedigree that includes ICPs such as Napster and Pirate Bay. Successful ICPs such as YouTube, push content controls to users, which has been a thorn in the side of content owners who want to be the sole arbiters of that property. Net neutrality serves as a reminder that companies, such as Time Warner, are both content owners and ISPs.[93] Such corporate convergence without net neutrality would allow these companies to constrain ICPs from both directions in the layer stack. Such corporate convergence can create new sources of regulatory power as diversified companies seek to leverage different mechanisms to maximize profitability and filter out the competition.

Public Code

Public spaces are coded. As an example, Lessig cites the Americans with Disabilities Act, a law that recoded public space in order to increase access.[94] Similarly, newly constructed public and private places must be built "to code." Building codes ensure a number of different things: they ensure compatibility between structures and public utilities such as the electrical grid; they ensure safety by describing construction techniques that will give the building the required structural integrity, and these codes also enforce certain types of spaces. Helen, GA is an example. Helen, GA is a small tourist town in the Appalachian Mountains of Northeast Georgia. It has all the amenities of a vintage tourist town from an age when road trips were forced down winding highways: restaurants, including fast food chains, mini-golf, wine shops serving local rotgut, and motels for weary travelers. Popular with bikers on long mountain drives and summer camp field trips to "tube the Hooch," Helen sounds like numerous other outposts across Appalachia, but Helen looks different. Specifically, Helen looks like a Bavarian village lifted out of Germany – even the McDonald's conforms to the aesthetic. Helen uses its building code to transform itself into a particular type of public space, which is designed to structure an economic space built around tourism. The building code enforces architectural predictability in both the public space and the private commercial space.

ISPs and ICPs own and operate networks on the network of networks. To extend the 'information superhighway' metaphor, these are the private spaces that you see as you drive along the highway. They consist of businesses with their doors open to the public, and businesses that are closed to all but those authorized to enter. Additionally, there are mom and pop stands, yard sales, and other roadside attractions. There are also private residences that remain closed to the public, and churches that are open to all. As you drive, though, you are in public space. You are on a road, that is maintained by a public authority for the public good, but this authority is not a government authority enforcing local zoning standards.

Public space on the Internet is most visible at both the logical layer and the applications layer. These layers are where interaction points proliferate, but those interaction points must be architected. This has led to an interesting assortment of entities that maintain this public space through standardization procedures that are meant to ensure many of the same things building codes accomplish, namely interoperability, stability, and maintenance of the public space. Standardization is the means through which these entities work to structure the parameters of online interactions, because standardization makes architecture predictable.

Standard setting bodies are by no means an innovation. Government and commercial standards settings bodies have always been a feature of market economies. Government interest in setting such standards is in the maintenance of public space. While commercial interests are often vocal in the standards adoption process, they can be met with skepticism when they become the arbiters of rights within the public space. As already established,

states only have partial control of the public space of the Internet, so as the state's territory runs out, a different type of self-regulatory body has stepped in: Internet Governance Communities (IGCs).[95] These governance bodies are self-regulatory in nature, and are marked by various levels of open membership that allows anyone with an interest and sufficient technical skill to take part in their deliberations. IGCs have grown organically with the development of Internet technology, and they constitute a community in which standard technical structures are negotiated.[96] Unlike the ITU, which has been unable to extend its regulatory power over Internet protocols, IGCs routinely adopt standards that affect functionality across all layers of the Internet. IGCs will be central to the analysis found in Chapter 7, but two brief examples are offered here as illustrations.

The heart of the protocol stack, the logical layer creates a public space through its open code. It facilitates the digital handshake between devices on the Internet, and the open standards that create the logical layer allow entities to set up shop on the information superhighway. The standards that facilitate such interoperability need to be open, nonproprietary, and accessible, and they must work well enough to ensure wide adoption, which facilitates architectural predictability. These standards are developed by the Internet Engineering Task Force (IETF). The IETF was established by the researchers initially developing the Internet, and "probably has the largest influence on the technologies used to build the Internet" despite its lack of "formal authority."[97] Originally a group of computer scientists hailing from universities and making contributions to the early network architecture, the IETF now allows anyone to join and take part in deliberations on its non-binding standards.[98] Though non-binding, these standards are adopted under a decision procedure that emphasizes "rough consensus and running code," a deliberative stance that values agreement and functionality equally.[99] The IETF places great emphasis on transparency in decision making, and it's essential "read me" document states explicitly a rejection of "kings and tyrants."[100]

A second example is the World Wide Web Consortium (W3C). The innovation enabled at the logical layer means that other public spaces can be opened in Cyberspace through the use of the applications layer. As examined before, WWW is an applications layer code, and its basic language is HTML. Specifically, HTML enables the concept of hypertext, which allows connections to be made among digital documents, a function commonly called linking.[101] In order to facilitate such hypertext linking, HTML needs to be standardized and open. The W3C is the standards setting body that ensures the publicness of the WWW.[102] W3C describes itself not as an organization but as an "international community that develops open standards to ensure the long-term growth of the Web."[103] It too has open membership allowing both organizations and individuals to join, and its decisions are taken by "community consensus."[104]

Both of these examples exhibit key characteristics that make IGCs difficult to characterize in organizational terms, making their evolution as a governance mechanism significant to understanding the legal geography of Cyberspace. First, IGCs are a reflection of the distributed, open nature of Internet architecture. Their open membership schemes potentially distribute decision making globally, and their process is open in order to ensure goals of interoperability.[105] Second, as communities – rather than organizations – their decisions impose community values into architectural design. In IGCs, the public, as a collective, creates and maintains the code of public space.

Personal Code

The end-to-end network reduces barriers to innovation as does open code at the logical level. These innovative edges open up spaces in which individuals can act at a global level and change the nature of interactions in Cyberspace at the applications level. Both PGP and the Silk Road, discussed above, are examples of coders rewriting state regulatory power. These application layer codes inscribe new rules on the state's ability to control information using cryptographic technologies, or as one commentator claims, the user is empowered to "[c]reate the digital world, and with it, [one's] own rules."[106] The individual is given direct access to implementing innovations that can reconstruct the legal geography the user inhabits. The implication that the individual can directly regulate in Cyberspace is controversial at best, and many would outright reject such a notion. Alternate readings would likely suggest that the code deployed by these individuals will be the subject of criminal or commercial law. Such readings inscribe national jurisdiction around the individual as the subject of the law.

These readings are rooted in territory and overlook ways in which these technologies re-architect legal geography.

Applications extend to individuals the ability to be the arbiter of their own rights in terms of informational freedoms. They are an "arbiter" in the sense that they can effectively hide personal interactions and remove them from the legal geography of territory. The logical layer allows applications layer code to bypass the state jurisdiction. The user respatializes to a legal geography that exists outside of the state's territorial gaze. The user as coder chooses the values contained in the code that he or she writes. This means that some may use these technologies to assert a freedom of political expression, but others can imbue the right with more nefarious content such as child pornography or terrorism. Such uses will be the subject of Chapter 8.

WikiLeaks serves as a good example. WikiLeaks is more than just a webpage. It is applications level code that allows individuals to send information to WikiLeaks while preserving anonymity.[107] Developed and deployed by Julian Assange with the help of a handful of other programmers, WikiLeaks became a global actor after it published a number of prominent leaks. This media attention peaked with the publication of thousands of State Department cables leaked by Chelsea (formerly Bradley) Manning.[108] Two things are important here, first Julian Assange's purposes for developing WikiLeaks specifically to invoke changes in world order and, second, the re-empowerment of the individual.[109] WikiLeaks is "a platform, a tool, an instance of technology," but it has an explicit legal purpose of diminishing the state's enforcement jurisdiction by reducing "incalculable legal costs" by transporting leakers to a new legal geography.[110]

The second thing to note is the power of the code. Cablegate leaker, Manning, was not caught as a result of the state following her digital trail. Instead, Manning revealed herself to a fellow coder, Adrian Lamo, who turned him in. Until that point, the United States had no evidence against Manning. Manning's own revelations returned her act to the interior of the legal geography of the state. Only when Manning spoke the crime did it materialize in a territorial sense.

—

The legal landscape of Cyberspace, as described above, is a multidimensional geography that can rewrite the jurisdictional patterns established as accepted in international governance. Multidimensionality is the result of the dual geography implicit in the layered architecture of the Internet. This reveals why the layered model carries force as an explanatory tool: through dissection of the network architecture, interconnected points of control can be identified and observed. The layered model facilitates "layered thinking," which can reveal how the spatial characteristics of Cyberspace can ripple across the conceptual stack and change other geographies, as has been shown in relation to the legal geography addressed above.[111]

The airport analogy that opened this chapter took us to an international frontier found in an airport's international arrivals hall. There is another aspect of this room that should be noted before moving to the final chapter in Part I. If you listen while in the arrivals hall, you can hear the muffled, a-rhythmic beat of stamps hitting passports. As observed above, jurisdiction, or legal geography, is usually mapped across space using a state's territorial borders as indicators of its limits. These borders represent another notion as well. In the airport arrivals hall, the border is as much about territory and law as it is about individual identity. The border is an expression of political identity, and passports are opened in order to check political identity. The next chapter will take up this notion through examination of political geography.

Notes

[1] Lessig, *Code 2.0* (2006) 38–60.

[2] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 184.

[3] *See* Bowman, "Thinking Outside the Border" (2007) 1192–95.

[4] Kulesza, *International Internet Law* (2013) 2–3.

[5] Johnson & Post, "Law and Borders" (1996) 1368.

[6] Akehurst, "Jurisdiction in International Law" (1972) 145; Schabas, *Genocide in International Law* (2009) 409; and Blount, "Jurisdiction in Outer Space" (2007) 299.

[7] Kulesza, *International Internet Law* (2013) 4.

[8] *See* Schmitt, *Nomos of the Earth* (2003) 42–44.

[9] *See for example* the cases of Adolf Eichmann: Arendt, *Eichmann in Jerusalem* (1963) 262–263; Augustus Pinochet, Roht-Arriaza, "The Pinochet Precedent and Universal Jurisdiction" (2001) 311–19; and Humberto Álvarez Machaín, Zaid, "Military Might versus Sovereign Right" (1996) 829.

[10] Kulesza, *International Internet Law* (2013) 6.

[11] Johnson & Post, "Law and Borders" (1996) 1368.

[12] Post, "Against 'Against Cyberanarchy'" (2002) 1373.

[13] Barlow, "Declaration" (1996).

[14] Post, "Against 'Against Cyberanarchy,'" (2002) 1368.

[15] *Id.* at 1381.

[16] *Id.* at 1375–76.

[17] *Id.* at 1373.

[18] Mattelart, *Networking the World* (2000) 1–13 and Werbach, "Breaking the Ice" (2005) 60.

[19] Luke, "The Politics of Digital Inequality" (1998) 125.

[20] Robertson, "The Suppression of Pirate Radio Broadcasting" (1982) 71–101 and Eppenstein & Aisenberg, "Radio Propaganda" (1979).

[21] *See* Lyall & Larsen, *Space Law* (2009) 256–269 and UNGA, Res.3 7/92 (1982).

[22] Post, *Jefferson's Moose* (2012) 60–89.

[23] Lessig, *Code 2.0* (2006) 300.

[24] Kulesza, *International Internet Law* (2013) 86.

[25] Post, *Jefferson's Moose* (2012) 164–71; Lessig, *Code 2.0* (2006) 294–97; and Kulesza, *International Internet Law* (2013) 107–08. A similar case is the German *CompuServ* case which addressed the availability of pornography via CompuServ services. *See* Kulesza, *International Internet Law* (2013) 106–107 and Lessig, *Code 2.0* (2006) 39.

[26] Kulesza, *International Internet Law* (2013) 107.

[27] The technology that led to the *Yahoo!* case predated technology that allowed for geolocation of users through their IP addresses. Kulesza, *International Internet Law* (2013) xiii. Debates on the geographic control of IP addresses persist Leiner *et al*., "A Brief History of the Internet" (2012); 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" (2014) 148; and ITU, "Resolution 133 (Rev. Busan, 2014) Role of Administrations of Member States in the Management of Internationalized (Multilingual Domain Names" (2014) 183.

[28] Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F. 3d 1199 (9th Cir. 2006).

[29] Kulesza, *International Internet Law* (2013) 103. *See also* Spar, "The Public Face of Cyberspace" (1999) 345.

[30] Post, "Against 'Against Cyberanarchy'" (2002) 1383.

[31] Johnson & Post, "Law and Borders" (1996) 1378.

[32] *See* Kulesza, *International Internet Law* (2013) 14 and McIntosh & Cates, "Hard Travelin'" (1998) 85.

[33] Habermas, *The Postnational Constellation* (2001) 63.

[34] Clapham, "Degrees of Statehood" (1998) 145 and Walzer, "The Moral Standing of States" (1980) 212.

[35] UN Charter (1945) Art. 2(4).

[36] Habermas, *The Postnational Constellation* (2001) 64.

[37] Sassen, *Territory, Authority, Rights* (2006) 54.

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

[39] *Id.* at 154–156.

[40] UNGA, Res. 37/92 (1982).

[41] Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline" (2014) I.D.35.

[42] *See* Codding, "International Telecommunications Union" (1994) 501. For other historical IOs *see* Mattelart, *Networking the World* (2000) 6–8.

[43] Constitution of the International Telecommunication Union (2010), preamble.

[44] *See* Codding, "International Telecommunications Union" (1994) 508.

[45] ITU Constitution (2010) Art. 12.

[46] *Id.* at Art 17.

[47] *Id.* at Art 21.

[48] Kulesza, *International Internet Law* (2013) xiii–xiv.

[49] *Convention on Cybercrime* (2004).

[50] Kulesza, *International Internet Law* (2013) 29, 60.

[51] Sofaer, Clark, & Diffie, "Cyber Security and International Agreements" (2010).

[52] Zalnieriute, "An International Constitutional Moment" (2015) 99–133.

[53] *See generally*, Power & Tobin, "Soft Law for the Internet" (2011) 31–45; Yannakogeorgos & Lowther, "The Prospects for Cyber Deterrence" (2013) 49–77; and Hurwitz, "A New Normal?" (2013) 233–64. *See generally* Finnemore & Sikkink, "International Norm Dynamics and Political Change" (1998) 887–917.

[54] *See* Kulesza, *International Internet Law* (2013) xiii–xiv and Hurwitz, "A New Normal?" (2013) 243.

[55] *See* Power & Oisín Tobin, "Soft Law for the Internet" (2011) 35. On uncertainty, *see generally*, Clark & Landau, "Untangling Attribution" (2010) 25; Libicki, "Two Maybe Three Cheers for Ambiguity" (2013) 27–34; Lessig,*Code 2.0* (2006) 25; McDermott, "Decision Making Under Uncertainty" (2010) 227–41

[56] Kulesza, *International Internet Law* (2013) 15 .

[57] *Id.* at 20.

[58] *But see* Betz & Stevens, *Cyberspace and the State* (2011) 107.

[59] *But see,* Kulesza, *International Internet Law* (2013) 69. *See also* the related concept of global public goods Stiglitz, "Knowledge as a Global Public Good" (1999) 308–25; Sy, "Global Communications for a More Equitable World" (1999) 326–43; Spar, "The Public Face of Cyberspace" (1999) 344–62; and Tambini *et al*, *Codifying Cyberspace* (2008) 10.

[60] Johnson & Post, "Law and Borders" (199) 1367; Kulesza, *International Internet Law* (2013) 124; and McIntosh & Cates, "Hard Travelin'" (1998) 114.

[61] *See, for instance*, Mattice, "Taming the '21st Century's Wild West' of Cyberspace?" (2013) 9–12.

[62] Tambini *et al*, *Codifying Cyberspace* (2008) 5.

[63] Lessig, *Code 2.0* (2006) 6.

[64] Tambini *et al*, *Codifying Cyberspace* (2008) 5 and Hayden, "The Future of Things Cyber" (2013) 4.

[65] "About Pong," www.ponggame.org (2016).

[66] International Table Tennis Federation, "The Laws of Table Tennis" (2016).

[67] Lessig, *Code 2.0* (2006) 5.

[68] *Id.* at 77–78, 124; Tambini *et al*, *Codifying Cyberspace* (2008) 11; Cass R. Sunstein, *Republic.com 2.0* (2007) 95. *See also* Eppenstein & Aisenberg, "Radio Propaganda" (1979) 155–56.

[69] Lessig, *Code 2.0* (2006) 110; Noveck, "Designing Deliberative Democracy in Cyberspace" (2003) 7.

[70] Lessig, *Free Culture* (2004) 123 and Lessig, *Code 2.0* (2006) 16. *See also*, Tambini *et al*, *Codifying Cyberspace* (2008) 11–12.

[71] Lessig, *Code 2.0* (2006) 24.

[72] *Id.* 84.

[73] Greenberg, *This Machine Kills Secrets* (2012) 148 (quoting Nick Mathewson).

[74] http://www.netflix.com.

[75] Streaming technology allows services to send only parts of a media file being actively watched to a user's devices, and it avoids local caching, so that the user's device does not retain the data that is sent.

[76] Rawls, *A Theory of Justice* (1971) 56.

[77] Bearman, "The Untold Story of Silk Road" (2015).

[78] Johnson & Post, "Law and Borders" (1996) 1388 and Kulesza, *International Internet Law* (2013) 60.

[79] Kulesza, *International Internet Law* (2013) 125.

[80] Greenberg, *This Machine Kills Secrets* (2012) 139–143.

[81] Tambini *et al*, *Codifying Cyberspace* (2008) 4.

[82] *For example, see* Gellman, "Civil Liberties and Privacy Implications of Policies to Prevent Cyberattacks" (2010) 273–309.

[83] Post, *Jefferson's Moose* (2012) 60–79.

[84] Burbank & Cooper, *Empires in World History* (2010) 153–162.

[85] For a salient example, *see* Saro-Wiwa, "On Environmental Rights of the Ogoni People in Nigeria (1995)" (2007) 360–363.

[86] Tambini *et al*, *Codifying Cyberspace* (2008) 30 and Jayakar, "Globalization and the Legitimacy" (1998) 726–29.

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

[88] *Id.* at 112.

[89] *See*, UN General Assembly, Res. 217 A(III). Universal Declaration of Human Rights (1948) Arts. 18 & 19; International Covenant on Civil and Political Rights (1976) Art. 19; European Convention on Human Rights (2010) Art. 10; and American Convention on Human Rights (1978) Art. 13.

[90] Osgood, "Net Neutrality and the FCC Hack" (2014) 33–34 and Verizon v. FCC (2014) 5–6.

[91] Rick Osgood, "Net Neutrality and the FCC Hack" (2014) 34; Verizon v. FCC (2014) 740 F. 3d 623 SLIP (Court of Appeals, Dist. of Columbia Circuit 2014) 6. *See also* Spar, "The Public Face of Cyberspace" (1999) 352; and Tambini *et al*, *Codifying Cyberspace* (2008) 8–9; Werbach, "Breaking the Ice" (2005) 78–9; Ranieri, "EFFecting Digital Freedom," (2014–2015) 52–53.

[92] Osgood, "Net Neutrality and the FCC Hack" (2014) 35.

[93] *See* Stout, "Comcast-Time Warner Cable Deal's Collapse Leaves Frustrated Customers Out in the Cold" (2015). *See also*, kliq, "Xfinite Absurdity" (2014) 51.

[94] Lessig, *Code 2.0* (2016) 127.

[95] IGCs is used to delineate these from IOs and to denote them as a distinct type of NGO (to the degree that they fit the definition of NGO).

[96] *See* Leiner *et al*., "A Brief History of the Internet" (2012).

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

[98] *Id.* at 129.

[99] Internet Engineering Task Force, "The Tao of IETF" (2012).

[100] *Id.*

[101] On hypertext see Brate, *Technomanifestos* (2002) 33–52, 220–225.

[102] Alvestrand & Lie, "Development of Core Internet Standards" (2009) 138–139.

[103] World Wide Web Consortium, "About W3C" (2016).

[104] *Id.*

[105] *See* Lessig, *Code 2.0* (2006) 148.

[106] Greenberg, *This Machine Kills Secrets* (2012) 148.

[107] *See generally*, Domscheit-Berg, *Inside WikiLeaks* (2011).

[108] *Id.*

[109] *Id.* at 160 (quoting Julian Assange as stating "I'm off to end a war" in relation to the Collateral Murder leak from the U.S. occupation of Iraq.)

[110] *Id.* at 174–75, 137.

[111] Werbach, "Breaking the Ice" (2005) 69.

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.