Network Geography: Cyber Landscapes

https://www.e-ir.info/2019/11/18/network-geography-cyber-landscapes/

P.J. BLOUNT, NOV 18 2019

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

"What difference does that make, what channel you got?" complains Ed Lindsay while he flips the stations on a television in a boarding house common room. Lindsay, a character in a 1961 episode of *The Twilight Zone*, is frustrated with the rapt attention that his housemates pay to the television. Soon after this exchange, Lindsay retrieves his 1935 console radio from the basement, and he finds that it receives, literally, broadcasts from the past. The radio's mystical power eventually transports Lindsay into the past for which he longs.[1] The episode, named "Static," avoids the usual, clichéd plot of fear of advancing technology coupled with eroding humanity, so often found in science fiction.[2] Instead, it makes a more subtle point about technology that is implicit but often overlooked in these narratives, namely that technology shapes the social experience of time and space. Though a permutation of the same broadcast technology, the TV world has different spatial and temporal reference points than does the world of radio. This can be seen in Lindsay's characterization of a musical performance on TV as "ruining a perfectly good song." The values imposed by the TV (video) are different from the values imposed by radio (audio). This is more than just an issue of production quality; it changes the interactions of the individuals within those spaces. Television's visual values prompt Lindsay to refer to his housemates as "hypnotized" as they watch. This is different from the space of radio, which created an interactive social space around its speakers, so when Lindsay reconstructs his space to the 1940s, the radio is not the focal point in the room, instead the focal point is his love interest.

At the surface, this fictional tale is wrapped in a narrative of social fragmentation caused by mass media, but beneath this narrative lies a deeper theme that sits at the heart of inquiries into modernity: the effects of technology on the construction of social space. What Ed Lindsay observes is that, though analogous, these technologies each change how the world around him is ordered in unique ways. They literally shape the space of the boarding house.

Cyberspace, as a technology, is no different. It shapes space, and it does this because the technology creates unique spatial orientations. The goal of this chapter is to describe the spatial geography of Cyberspace in terms of its technical manifestations, and in terms of the dominant conceptual narrative through which Cyberspace is understood. This description will resist adopting a definition of "Cyberspace" in absolute terms. Part of this impetus comes from the diverse definitions that already exist in the literature describing Cyberspace, but never in complete terms.[3] As a result, the chapters in Part I will focus on describing Cyberspace to facilitate a richer understanding of its contours. This approach flows from a central hypothesis that Cyberspace is a geography in which social relations unfold. Description is thus prioritized over definition due to the difficulty in defining a dynamic space both accurately and coherently. Definition is a tool to simplify concepts. Description, on the other hand, reveals nuance and complexity critical to a rich understanding, as sought herein.

This chapter will first use a layered model to describe the technical architecture of the Internet, which is distinct from Cyberspace. Once this technical space has been articulated, the spatial conceptualization of Cyberspace will be explored. Section II of this chapter argues that the dominant human understanding of Cyberspace is through a spatial narrative, and that this narrative has powerful implications for the social conceptualization of Cyberspace. Finally, the chapter will conclude by examining the inhabitants of Cyberspace and the implications of networked

populations. The spatial geography of Cyberspace is critical to understanding the larger thesis that Cyberspace recodes borders and reprograms the world.

Networked Space

Ed Lindsay's question of "what does the channel matter" can be answered easily: a lot. The technology of TV is such that choosing a channel means choosing a network – and choosing a network means accepting the content chosen by the network. Changing the channel changes everything, and it was the only way to change the output of the TV. The networks accessible on a given TV are limited by location since broadcast TV is a function of proximity to the transmitter. Furthermore, accessibility was limited to reception from the broadcaster, but not interaction with the broadcaster. The space that TV creates is one of viewers relegated to peering in.

If "Static" were updated for contemporary airing, one could imagine the boarding house crowd all gathered in the common room, but the focal point would be their own personal electronic devices. Ed Lindsay, instead, would yell because they were not taking part in the social act of watching the TV in the common area and building community through the shared experience of viewing. While Lindsay's technological skepticism would be built on substantially the same rhetorical claims, the space in which he would be making his claims would be very different. In this updated version, each individual would be focused on being in Cyberspace and, importantly, interacting with others in Cyberspace. Each individual will have chosen their own channel. Some of these channels, such as services like Pandora or Netflix, mimic previous information technologies. Other channels create vastly different opportunities for engagement and interaction. Indeed, many individuals in this alternate take would be interacting with more individuals as a result of this technology. This simple shift changes the constitution of the common room space, because "the Internet is not like TV – you use it, it doesn't use you."[4]

Technology, in particular information technology, changes human interactions.[5] This is because these technologies are capable of providing more and richer information, and information sits at the core of social interactions. Space is constructed by human technology, and humans experience spaces differently depending on how technology is deployed. Ed Lindsay experiences the common room of the boarding house differently when different technology is deployed. This is similar to trends noted by Cohen in which surveillance technologies alter public space. Surveillance technologies, beyond simple observation, achieve "the active production of categories, narratives, and norms."[6] Cohen argues that these technologies change space by "constrain[ing] the range of available behaviors and norms."[7] Surveillance technology is emblematic of how the "prolifera[tion]" of "transaction points" changes the experience of physical geography.[8]

Before abandoning a happy Ed Lindsay in the 1940s, we should take a closer look at the nature of the technology that is defining the space in which he lives, or more precisely defining his transaction points. Mass communication in this world is the product of centralized, one-way communication. In this model, power is located at a central position, and is understood as the power to transmit. The entity that controls the transmitter also controls the content that the viewer or listener sees. The end device only receives; none of the knobs or buttons allow the user to send a message back to the transmitter. Mass media in this space is about transmission to the masses that receive it.[9] It is a one-way street, and the space at the receiving end of that street is shaped by this technology. The Internet dismantles this one-way paradigm and presents the user with an array of opportunities to engage in multi-way communication with other individuals, with the masses, and with nearly any other type of entity capable of communication. This fundamental difference creates dramatic changes for the nature of human interaction and social order, because transaction points become myriad and are distributed worldwide.

It is important to note that the Internet is distinct from Cyberspace. The Internet, for present purposes, can be understood as the technology that makes Cyberspace possible.[10] The technology of the Internet facilitates and is inseparably entangled with the phenomenon we know as Cyberspace, which inhabits broader social dimensions. This means that in order to describe Cyberspace, one must first describe the Internet.

A layered model is adopted herein to explain the technical architecture of Internet. This model "was developed by computer scientists to explain the functional components of the Internet and how they work together to convey

Internet traffic."[11] A number of legal scholars have adopted the layered approach to explain policy and regulation on the Internet.[12] While these regulatory aspects will be explored later, at present the layered model presents a useful model for breaking down the component systems that work in concert to make the Internet possible. The layered approach is a "conceptual tool" that "divides a networked information system into a hierarchical 'stack,'"[13] presenting the Internet as a combination of different technologies with different functions stacked together to form the whole. This approach is useful, because the "interconnectivity among networks" is "so complex that it is not easily understood."[14] Layering creates a model for categorizing diverse, yet interrelated, technologies by function and reveals how each "self-contained" category is linked to the layers above and below it.[15]

Different authors have used different stacks of layers. For instance, Post simplifies the Internet into two distinct layers, the network layer and the applications layer[16]; Kulesza uses three layers[17]; whereas Solum and Chung use a six-layer stack (See Fig. 1.1).[18] The differences in the models are not substantive in nature and are, instead, based on the resolution of the analysis of the "conceptual tool."[19] A medium grain four-layer stack will be used here to avoid both oversimplification and unneeded complexity. Werbach and others have identified a four layered stack, which contains a physical layer, a logical layer, an applications layer, and a content layer.[20] This four-layer stack will guide the analysis here.

The Physical Layer

At the bottom of the conceptual stack is the physical layer. The physical layer is made of the hardware on which the Internet runs. This hardware consists of routers, servers, cables (copper and fiber optic), cell towers, satellite links, and other telecommunications technologies.[21] This infrastructure is essentially the connective tissue of the Internet, providing the medium through which information is transmitted. The physical layer includes all the physical equipment associated with the Internet. This importantly includes the Internet backbones and telecommunications networks, which provide the physical means through which data flows.

Internet backbones are a group of services providers that connect to route information transfers between

autonomous networks.[22] These providers sell internetwork connectivity access to other providers who provide services to third parties such as individual users or corporations.[23] This secondary set of providers are commonly known as Internet service providers (ISP). An Internet backbone

essentially forms its own network that enables all connected end users and content providers to communicate with one another. End users, however, are generally not interested in communicating just with end users and content providers connected to the same backbone provider; rather, they want to be able to communicate with a wide variety of end users and content providers, regardless of backbone provider. In order to provide end users with such universal connectivity, backbones must interconnect with one another to exchange traffic destined for each other's end users.[24]

Backbones route the flow of information among networks. It is important to note that their function is only the transfer of data. Backbones do not store the information on the Internet; they transmit data among networks.

The backbone providers – and the providers to whom they sell – send data to users via telecommunications networks. For instance, most home users connect to the Internet via telephone wires or coaxial cable – both of which were installed to be used as a medium for different technologies. But users can also connect to the Internet via cellular networks, radio frequency or Wi-Fi, or through dedicated lines. Two things should be noted at this point. First, the Internet is running on a diversity of networks that deploy different connective technologies. This means that it facilitates a high level of interoperability among diverse technologies. Second, these networks are owned by a diverse group of actors, meaning there is a high level of interoperability among entities. The Internet's functionality is centered on this technological ambivalence towards the medium of transmission as well as the identity of the transmitter or recipient of the transmission. This is dramatically different from previous telecommunications technologies that were regulated according to the specific technological parameters that limited interactivity. For instance, broadcast was regulated according to principles that maximized the efficient use of the scarce electromagnetic spectrum, whereas telephone regulation was used to maximize public access.[25] Technological ambivalence is indicative of a trend that is visible at all layers of the conceptual stack: convergence. Convergence is a process through which the "historical distinctions between communications networks are melting away."[26] Convergence is a product of the logical layer, which is next in the conceptual stack of layers.

The Logical Layer

Convergence occurs at the physical layer because the logical layer re-configures how information is sent over the physical layer. The logical layer consists of the software protocols that define the data being transferred by the Internet. All telecommunications systems transfer data electronically, but traditionally this signal was analog and was limited by the strictures of the technologies that carried analog signals.[27] The advent of computers enabled digitization, which allowed for the same content to be encoded as standardized data or "fundamentally just a string of ones and zeros" that are "ultimately interchangeable, meaning any communications platform can in theory, offer any service."[28]

The heart of the Internet is the Transfer Control Protocol/Internet Protocol (TCP/IP).[29] This protocol sets the standards for transmission of data on the Internet. It defines two distinct functions. First, it defines how the information being sent should be packaged. Digital information, unlike analog information, is easily severed and reassembled. When information is sent over the Internet, a computer program on the end user's device will slice it up into small packets of data. Each packet is labeled with the order in which it should be reassembled. The second function the TCP/IP describes is the Internet protocol, which places a distinct address on each packet that tells nodes on the network where it should be sent. This process is known as packet switching.[30]

Packet switching revolutionized telecommunications, which to that point transmitted analog signals and depended on circuit switching. Every device on the Internet has an IP address, a numeric identifier for all traffic to and from that device, which is similar to a phone number.[31] Historically when a call was made on a landline, an analog signal was sent that required constant connection to a circuit to the other end of the call.[32] That circuit is connected through a centralized operator, a process known as circuit switching.[33] A visual of this process was a common feature of early

television programs, which would often use a split screen to show the operator physically connecting the continuous circuit on a switchboard with a patchcord. Packet switching on the other hand does not require a continuous connection because the information is broken into data packets instead of a continuous analog signal. This means that the packets can be routed via any combination of routes through the network in order to get them to the proper IP address. Instead of a centralized operator, there are decentralized routers and nodes through which a packet travels. This type of networking allows for more efficient transfer speeds by distributing loads across the network.[34] In other words, the packets do not need to travel along the same path or arrive in the same order, so packets are sent along the most efficient route possible. In practical terms this means that an email, for instance, once broken down into packets could travel through numerous different servers located in geographically disperse places. Packet switching avoids the strain on the central operator from which circuit switching suffers.[35]

A number of salient features of this system should be emphasized. First, the TCP/IP protocol is designed to transfer a packet regardless of the information it contains. Importantly, as currently configured, the routers on which the protocol runs do not register what is "in" the packet.[36] The router simply passes the packet along to the next waypoint on its journey. This is why the Internet is sometimes called "stupid."[37] The design of the Internet is simply to allow information to be freely transferred among the various nodes on the network meaning that the content of those packets is not stored in the logical layer.[38] Second, this means that the transmission of the data is neutral in regards to the technology on which it travels. The Internet can run over copper cable, fiber optics, electromagnetic frequency, or anything else that can carry electronic communications. TCP/IP provides a standardized manner for packaging and addressing data for transmission. Third, as a result of this technological ambivalence the Internet has the potential to be widely accessible. The Internet is not a single network, it is a network of networks facilitated through a standard protocol. The Internet, when viewed at the protocol layer facilitates the linking of dissimilar networks as data packets can ride on any telecommunication infrastructure.[39] Finally, since the standard protocol is meant to ensure interoperability, the network itself is rhizomatic in nature inasmuch as it is a non-hierarchical assemblage of networks.[40]

It was stated earlier that the logical layer functions as the heart of the Internet. This is because it serves as the vital link between the physical layer below it and the applications layer above it through an "open network architecture," which is the "key underlying technical idea" of the Internet.[41] Open network architecture provides a link among disparate physical layer technologies and disparate applications layer technologies by creating a common language of communication *among* them as opposed to *between* them.[42] The logical layer drives convergence at the physical layer because of these attributes, but this convergence is experienced at the applications layer.

The Applications Layers

The statement that the Internet is "stupid" is based on the logical layer's functionality to be non-discriminatory in the transferring of data packets and is commentary on the popular conceptualization of the Internet as a vast archive of knowledge. The Internet is "stupid" because it is an end to end network, which means intelligence is "vested in the edge."[43] The devices and applications they run at the edges of the network are where the Internet "happens," so to speak. The data packets that the logical layer transmits are only intelligible at the ends of the network, because "the Internet . . . was not designed for just one application, but as a general infrastructure on which new applications could be conceived."[44] Essentially, to use a buzz phrase ushered in by smartphones, "there's an app for that."

The World Wide Web (WWW) serves as an excellent example. If asked "what is the Internet?" many people would likely describe it as the WWW as this is still one of the most common ways that people experience the Internet.[45] The WWW is actually an application that runs on a device and functions at the applications layer.[46] A rudimentary explanation of how the WWW works will help to show how the applications layer functions as well as the end-to-end principle. If you want to view a web page you type a Uniform Resource Locator (URL), for instance http://www.dudeism.com, into your web browser's address bar.[47] The first thing to be noted is that there are multiple web browsers made by a variety of entities including corporations, non-profits, and individual programmers. The web browser then sends a request via your Internet Service Provider (ISP) to a server that contains a file with a list of URL's associated with the .com root name.[48] It searches this list, called a root file, for dudeism.com, and finds the IP address of the device that is associated with dudeism.com through the Domain Name System (DNS). In simple

terms, 'dudeism.com' is a text-based identifier for the IP address, which is 64.91.245.254 (as of this writing). The ISP, on your behalf, then contacts this device, which has been configured to act as a server,[49] and looks for a directory named "www." Once there, the browser will look for a default file, most commonly titled "index.html," and the ISP will transfer a copy of this file, which your computer downloads.[50] A copy of the file named index.html now exists on your computer, and your browser opens this file, which contains computer code that a web browser understands and executes. This code tells the browser what to display on your screen. This entire transaction is facilitated by the logical layer and is transferred as digital electromagnetic signals across the physical layer.

In this example, we can see very clearly that the information that we access while connected to the Internet is stored at the periphery. The web page is not "on" the Internet, rather it is accessible via the Internet, and it exists on a connected device. The file that you see is copied to your computer, meaning that information from afar becomes immediately localized, even if temporarily, in the memory of the user's device so that it can be manipulated by the software on that device.[51] This is the end-to-end principle in practice, which is "hard-wired into the Internet's architecture."[52] In technological terms, this is known as "peering."[53] Peering implies equality created between devices through the common protocol. Of course, this is equality in technological terms only and not be confused with equality in a legal or political sense.

A practical effect of the end-to-end principle means that convergence is experienced by the user at the applications level. Indeed, the "there's an app for that" catchphrase captures this very idea. Convergence is experienced because information can be digitized, and technological ambivalence facilitates a diversity of applications with different outputs. This has resulted in a bloom of technological innovation as applications and networks have proliferated.[54] Possibly the best example is the Internet of Things (IoT) concept in which devices other than traditional computers are being networked for applications such as home automation. IoT allows nearly any machine that can be manipulated by a circuit board to be networked into the spatial geography of Cyberspace. So, for example, there are now lightbulbs on the Internet.[55] Innovation at the applications layer is further driven by the decentralization of the logical layer, which gives more individuals access to information systems.[56]

Another reason that innovation happens at the applications layer is that in order to facilitate interoperability of networks, the protocols of the logical layer are open, allowing anyone with proficient skill in programming to be able to write an application that facilitates new types of information flows. This significantly lowers the cost of development of new products, but it also means that individual programmers can change how Internet communications work – or more precisely change the nature of communications through the applications layer. A good example is Phil Zimmerman, who wrote the Pretty Good Privacy (PGP) program. This public key encryption program was developed to allow users to send secure encrypted messages to other individuals via the Internet.[57] Interestingly, encryption programs like PGP are classified as weaponry under the US International Traffic in Arms Regulations (ITAR).[58] These regulations restricted the export of PGP as a defense article.[59]

The example of PGP illustrates three important things that will be seen in a variety of contexts within this research. First, a single coder changed the nature of Internet transactions. This means that a single individual, taking advantage of the innovation-friendly nature of the end-to-end network, was able to change the possibilities for human interactions on the Internet and in Cyberspace. Second, this technology was unable to be contained by the state. ITAR is specifically directed at the export of weapons technologies that appear on the United States Munitions List (USML). These regulations apply to technology crossing the border of the United States, yet PGP was freely available worldwide soon after its creation, indicating a breach of the space of the state. This availability is driven in part by the ephemeral nature of software, which is easily shared online. Finally, this application, for the purposes at hand, cannot be imbued with normative power. The descriptive bent of this chapter requires that PGP, like all programs at the applications layer, be recognized as a technology that can enable good interactions (e.g. giving voice to political dissidents in repressive regimes) as well as bad interactions (e.g. giving cyber criminals the ability to transmit illicit data free from scrutiny). The innovation facilitated by the applications layer is such that it creates openings for all entities – whether they be normatively good or bad; state or non-state; commercial or criminal; individual or collective – to engage in a variety of measures of control and liberation.

The Content Layer

Content is what concerns most people using the Internet. They neither care to know nor need to know the specifics of the code that is running beneath the content layer at either the application or logical layer. Nor do they likely understand the intricacies of the physical network past their connection to the ISP. They are concerned with content, and in a digital world, content can be just about anything. While sights, sounds, and words have been the traditional domain of the Internet, in no way is the Internet limited to transferring only these types of information.

The Thingiverse website is an online repository of 3D printable objects.[60] Or more precisely, it is a repository for programs that will instruct a 3D printer to print a specific three-dimensional object. The object itself is not sent through the Internet, but the effect is the same since the object materializes at the user's device. Essentially, if hardware can be developed that can output a type of information digitally at the applications layer, then that data can be transferred across the Internet. The output of end devices is the content layer.

The content layer is, obviously, the layer where most of the public debate on Internet regulation occurs. This is because the interaction of the three layers below the content layer allow for large amounts of data to be transferred quickly to anyone no matter where they are so long as they have network access. The content layer of the Internet is dramatically different from the content layer of previous telecommunications sources, which disaggregated different functions. Broadcast is a one directional method that reaches mass numbers of people, whereas the telephone allowed for bidirectional interactions but not on a mass scale. The centralization of broadcast made it easily susceptible to societal controls over the content whether through regulations or norms. The telephone, on the other hand, offered little control over content, but architecturally minimized the possible reach of the communication. Content on the Internet is both multidimensional and mass, meaning there is low control over the content and the reach of information. This can most clearly be seen in the concerns that numerous states have about content coming in through their borders such as political propaganda or pornography.[61]

Much of the discussion around Internet governance focuses on issues of free speech and censorship centering debate on the content layer. This is because the three underlying layers in concert amplify traditional societal concerns with flows of information. Information now flows across networks that are distributed in nature, permeate borders, and maximize access by individuals. This is a paradigm shift in telecommunication technology, and its effects on society are broad. The content layer is the locus of these effects, as it is the content – whether the content is in the form of economic activity, religious ideology, political activism, or criminal conduct – transmitted via the Internet that creates societal issues.

Cyberspace

A genre of movies and songs from the late 70s and earlier 80s celebrate the culture of Citizen Band (CB) radio. In particular, the film catalog of Burt Reynolds is notable with *Smokey and the Bandit* (1977), *Smokey and the Bandit 2* (1980), *Cannonball Run* (1981), and *Cannonball Run II* (1984). Aficionados might also appreciate television series such as *The Dukes of Hazzard* (1979–1985), *B.J. and the Bear* (1979–1981), and *Movin' On* (1974–1976), and country music offered up a plethora of songs such as C.W. McCall's "Convoy" (1975), Red Sovine's "Teddy Bear" (1976), and Cledus Maggard's "CB Lingo" (1976). These cultural nuggets give a glimpse into a culture built around a network of people that interact on CB radio channels. In these narratives, news often spreads quickly across the network leading to collective group action, which usually finds expression in highway hijinks. The CB goes hand in hand with the automobile as both served as potent symbols of individual autonomy (and it is likely no coincidence that these narratives often glorify running from the law enforcement in high speed chases). One of the most notable things in this genre is that the CB has its own language that socializes the participants in the network. CB in these films is portrayed as more than just a communication technology. Instead, it is the glue that structures the social space of mobility-driven culture.

If the Internet is a stack of functional layers, then Cyberspace is the Internet with the addition of a social layer.[62] This may seem a little obvious. After all, the Internet is not a natural phenomenon and is a human creation, meaning a social layer may be presupposed. While true, the point here is to highlight something more than just human usage of the technology. It is, instead, to highlight the scope and integration of the Internet into societies globally. The social layer creates a "structure of metaphors and visions" that conceptualize the space that the Internet creates.[63] The

technology of CB radio still exists and is used, but when was the last time that a story about human activities on CB topped the news? The reason for the dearth of media coverage of the CB network is that much of the social layer has been removed as CB was supplanted by cellular phones, which better served most people's needs. The drop in scale of usage means that the network has less importance.[64] It is precisely the fact that 48% of the world's population is connected to the Internet and this number is rapidly growing that makes Cyberspace an important social phenomenon.[65] Social interactions of all sorts are taking place there, but where is there?

This section will first establish that a spatial narrative serves as the dominant conceptualization of Cyberspace. Then it will probe the attendant metaphors to this spatial narrative and attempt to identify Cyberspace in terms of location and place.

Cyberspace as Space

A great deal of the early literature on Cyberspace debated specifically whether it constituted a new space distinct from the space inhabited by states. The legal debate, focused on the multijurisdictional effects of Cyberspace, is best exhibited in the scholarly exchange between Jack Goldsmith and David Post. Goldsmith argues that Cyberspace presents no novel legal problems, and that "Cyberspace transactions do not inherently warrant any more deference by national regulators, and are not significantly less resistant to the tools of conflict of laws, than other transnational transactions."[66] Post on the other hand, a self-proclaimed "cyberexceptionalist," argues that Cyberspace should be approached as a new geography that humans inhabit. At the heart of this debate is one fundamental issue: is cyberspace a space?

Goldsmith's answer to this question is that since Cyberspace exists on the Internet, then Cyberspace exists where the physical links and users do. The physical layer and users exist within physical territory of the state. Through this lens Cyberspace only has a "space" to the extent that its physical components do. Post on the other hand would argue that something fundamentally different is happening, because Cyberspace mediates the vast number of human interactions without regard to the physical and political boundaries of the terrestrial sphere.[67] He argues that the difference between real space and Cyberspace is akin to the difference between "life on land" or "life in the sea."[68] In this model, Cyberspace's spatial dimension is defined by the entire layer stack, and not just the territorially grounded physical layer.

The problem is that, to some extent, both authors are correct. Most of Cyberspace's physical manifestations do exist within state borders. Thus, a regime such as that in North Korea can control the spread of Cyberspace by maintaining tight controls on the dispersion of physical technology at its borders – leading activists to attempt to send in technology using balloons.[69] Cyberspace, at the same time, defies containment by the state and seemingly exists everywhere. The Pirate Bay, a prominent torrent website carrying links to copyrighted material, has repeatedly evaded being shut down by state power structures through the use of mirror sites, which disperse the site across servers in various geographic regions.[70] The reality is that Goldsmith's argument while logically solid is often "more honoured in the breach than in the observance."

One of the problems with Goldsmith's view is that it ignores a simple fact: humans understand Cyberspace as a space. Cyberspace is conceptualized as space through a spatial narrative that serves as a dominant metaphor for human understanding of Cyberspace.[71] In other words, Goldsmith "presuppose[s] a hard division between a regulated physical layer and everything else."[72] Goldsmith's argument seems facile when applied to the Internet, but it becomes dissonant when applied to Cyberspace. This is because the spatial narrative makes technological reductionism impossible, as "the way we describe a thing can change the nature of that thing."[73] The spatial narrative that accompanies Cyberspace is very much a description of social experience in Cyberspace.[74] The spatial narrative "transform[s]" the "experience" of Cyberspace."[75]

The spatial narrative is found within the common vocabulary used to describe Cyberspace. Users go *on*line and visit chat*rooms* or web*sites*. These can be found by typing in an IP *address* that is often denoted by a Uniform Resource *Locater* (URL) which includes a *domain* name. That name is understood to be *owned* by an entity, which will probably have a fire*wall* up to keep intruders out of its *local* server. Lessig notes that "cyberspace is something you

get pulled 'into.'"[76] Ferguson and Mansbach note terminology such as "electronic highway, electronic mail, infobahn, infosphere, … information superhighway … online community, virtual community, and virtual reality."[77] Barlow's influential "Declaration of Independence for Cyberspace" declares that states have "no sovereignty" in the "new home of the mind."[78] Resnick refers to the "land of Cyberspace,"[79] and Post uses the metaphor of exploring a new territory to evaluate law in Cyberspace.[80] In short Cyberspace has a "placeness."[81]

This metaphor is central to the social construction of Cyberspace, because "metaphors have a profound effect on computing."[82] As the Internet reached more users, these concepts could often be found in the iconography of Internet Service Providers (ISP). For instance, America Online (AOL) was one of the first mass market ISPs, and, as a result, AOL was the initial first online experience for a large portion of the Internet users that flooded the Internet when it was privatized in the mid-1990s.[83] AOL used skeuomorphs to orient these new users. For example, the sound of an opening and closing door was used to denote entrance and exit of users from chatrooms. Similarly, an icon of a traditional roadside mailbox denoted the email server thereby linking the email concept to its physical counterpart, which would have specific geographic location denoted by a physical address. AOL is not an isolated example; skeuomorphs have been used extensively in digital design to help orient users.[84] The desired effect is the creation of a visual, spatial geography that new users can easily orient themselves using concepts associated with physical geography.

The pervasiveness of the spatial metaphor illustrates something very important that is often overlooked in Goldsmithian type arguments. No matter whether Cyberspace exists in a physical place, it is conceptualized and understood as a space by its users. Cyberspace is experienced as space, and it is "different from real space."[85]

Cyberspace as a Place

If Cyberspace is a space then where is it? Space is intrinsically linked to the idea of location. Locating Cyberspace is a difficult task, and the spatial narrative can only be pushed so far.[86] Part of the problem is that an individual can never be wholly in Cyberspace, yet this has not kept Cyberspace from being understood in terms of spatial concepts. The Internet's layers, discussed above, construct the spatial geography of Cyberspace by setting the metes and bounds of human interaction online. In the same way that rivers and mountains create natural boundaries, Internet technology also creates boundaries for human interactions. The spatial metaphor invokes a number of important concepts that shape social understanding of Cyberspace.

Cyber-realists will claim that Cyberspace is located within the physical bounds of the state. For instance, in terms of the WWW, URLs denote a specific server on the Internet, which does exist in a physical location and is owned by an entity. The URL is conceptually very similar to the idea of an address, which denotes a specific geographic location, so the URL points to a place with a location that is within the borders of a state, and to a specific *res* within that state. This answer to the location problem is not without issues, though. URLs are freely associable to other servers that can contain either the same information or different information. The server itself may be static, but the website that is visited in Cyberspace is not. It can move with a simple change to the DNS root file, which will resolve the URL to a different IP address, and to a different *res*. The distinct *site* that the user *visits* is indeed fluid in a spatial sense. Cyberspace exists in a geographic duality. Like Papa Legba with one foot in the grave, Cyberspace has one foot firmly planted inside state borders, but the other foot is planted somewhere outside those borders.

The spatial narrative is a social conceptualization that renders Cyberspace as a "distinct 'place.'"[87] As a place, it exists concurrently yet separately from the state, meaning it both borders and intersects the state. Because Cyberspace has transnational effects that are unbounded by physical geography, it is submitted here that Cyberspace constructs and is located in a global space.[88] A global location implies two things. First, Cyberspace is a space with world scale, and its growing level of integration into societies worldwide is hardly deniable. Second, Cyberspace is a geography that is exterior to international space. The network architecture that underlies Cyberspace allows it to evade the strictures of national borders. Global space is located where internationally defined territory thins and runs out.

To understand this, one must first recognize that the concepts of space and location also implicate further notions

such as borders and property. The often-quoted trope from the early days of the Internet that "borders are just speed bumps on the information superhighway" points directly to Cyberspace's spatial character and global location. Indeed, the spatial metaphor of a highway is a reminder that all the locales in Cyberspace exist in the same place, or maybe better stated, they all have addresses on the same street. All IPs on the Internet are equally close to the user. While the ability of states to raise borders in Cyberspace is not completely absent, the user's ability to thwart those mechanisms allows for penetration of those borders at will, showing that software borders are indeed soft. The rhetoric of the spatial narrative supports this. For instance, John Perry Barlow's "Declaration of Independence for Cyberspace" declares explicitly that "Cyberspace does not lie within [a state's] borders."[89] Barlow is linking the independence of Cyberspace to its own territorial sovereignty, stating later that he "felt like the answer to sovereignty was sovereignty. To fight them on their own terms."[90] The spatial narrative gives conceptual credence to extraterritoriality of Cyberspace.

The concept of property is also implicated. The Western norms of ownership and exclusion are set on end in Cyberspace, which "makes a hall of mirrors out of conventional understandings of what constitutes private and public property."[91] Take the website example used above. Users often reference ownership of a website, but this is inexact at best. What these users are describing is two different phenomena of "ownership." First, they are describing the URL which indicates location of the website, but this domain name is only registerable and not owned so an individual's rights in it do not represent traditional property rights. While entities may own intellectual property rights to attributes of the URL,[92] they must maintain their registration in order to keep the URL, whether they use the URL or not. Interestingly, this means that it is possible to register a URL to keep it from becoming a place in Cyberspace. Furthermore, the URL can easily be pointed to another server by associating it to a new IP address, meaning that the URL as an owned space is to some extent ephemeral. This points to the second phenomenon of ownership that users are describing when they discuss ownership of a website, which is ownership of the content that is displayed in the browser window, which can be thought of in terms of intellectual property.[93] Since the webpage is available worldwide, questions about the territory that protects those intellectual property rights arise. This becomes messier when one takes into account that a great deal of web content is copied and stored on the local machine, and when one contemplates that the success of social networking websites is often predicated on serving content that is sourced from somewhere other than the website's "owner." Interestingly, a third concept of ownership is not usually invoked when referencing website ownership, which is ownership of the server in the physical layer, where the cyber-realist focuses their analysis. This type of ownership is diminished in importance since a URL and data can be moved to new servers at will, meaning that the physical location changes fluidly.[94] Additionally, the entity that places the content on the server often rents that server space from a third party and has no physical control over it further muddying the ownership waters.[95]

The website example hints at the underlying issue for property narratives in Cyberspace: hard physical location is ephemeral because property in Cyberspace is practically infinite. Western understanding of property is predicated on scarcity, which rests on the idea that "they aren't making anymore of it." In Cyberspace, property is fragmented across physical space and metaphysical space resulting from the effects of the logical layer which makes data fungible such that it can move freely from place to place and exist simultaneously in all those places. Property in Cyberspace expands simply by adding devices with computer memory to the network, or by adding new files to established servers (e.g. adding a new post to a blog).[96] Notions of property based on scarcity and ownership become tenuous as scarcity decreases and ownership fragments.[97] So, for instance, scarcity of land is central to Schmitt's conception of the land generating the law – as it is the scarcity of land that drives its division. However, when territory is infinite the need for division is functional as opposed to economic. This is not to argue that there is no economic value in domain names, but that value is derived not necessarily from scarcity, but from the idea contained in the domain name, which is most often linked to the name recognition associated with a company or brand. Thus any URL, in theory, has the potential to be of high value if it achieves high recognition, whereas real properties value is linked to physical attributes.

None of this is to say that traditional notions of borders and property do not still have sway. As noted earlier, Goldsmith's observation of physical location granting state's territorial control over Cyberspace technologies is relevant, because users are "always in both places."[98] This, however, is only part of the story. States can only control the parts of the Internet they can literally touch, but not necessarily all the parts of the Internet that can touch

them. The technological landscape that intersects state territory is architected in such a way that much of Cyberspace is located outside the state.

Metaphysical Geographies

The critical notion in this chapter is that Cyberspace is understood by humans as a space and as such it also has location and place. Despite its metaphysical nature, individuals cannot help but envision Cyberspace in terms of its spatial characteristics. This is no surprise to anyone familiar with the literature on Cyberspace, which struggles with the ethereal nature of a place that is both there and not there in the sense of "traditional dimensionality."[99] Indeed, the concept of virtual reality embeds the spatial narrative quite deeply into understandings of Cyberspace. At its inception, virtual reality was portrayed as the ability to go into a new space and to experience it as real.[100] This concept materialized in applications such as Second Life, which allowed a user to explore and interact in a virtual world that was created by the individuals that inhabited it.[101] Virtual reality's current inception through devices such as Microsoft's Hololens allows the users to visit virtual spaces as well as real spaces.[102] Additionally, led by the pornography industry, devices are being created that allow for a richer level interactions of individuals in Cyberspace.[103] These technologies move beyond an audio/visual experience in Cyberspace and allow users to take part in the experience portended by AT&T's 1980s ad slogan "Reach Out and Touch Someone."[104] The ability to physically "touch," even through an Internet connected device means that the metaphorical has become the experiential. Physicality is now freely transportable beyond borders, which become much less benign in an example like Stuxnet where code was used to physically and surreptitiously manipulate centrifuges in an Iranian nuclear facility.[105] Cyberspace cannot remove a mountain in between two places, but it can render many of the mountain's effects irrelevant.

The idea of touch leads to a final observation that must be made about Cyberspace: as a space it has inhabitants.[106] Granted these individuals live both in Cyberspace and out. There is developed rhetoric that refers to netizens and cybercitizens, both of which implicate a core concept of citizenship that is traditionally linked directly to territorial authority.[107] Arguably the term "global citizen" found in the literature on global governance can only be conceptualized with a technology that can free the individual from the strictures of their national citizenship. While such ideas might be dismissed as purely rhetorical, we can see that they indeed do have manifestations such as Estonia's e-Residency campaign, which extends digital rights to registered entities.[108]

Digital natives may be the most potent of these metaphors for inhabitation, as society has not yet entered a time in which individuals have no concept of what it is like to not be contained within networked space. Digital natives, a naturally rising part of the population, will not conceptualize spatial organization without the inclusion of Cyberspace. Rhetorically, the term 'digital natives' indicates that these individuals are more than just transitory surfers. Their geographic experience will always be networked and machine mediated. In such a world, a digital-self existing on the network becomes a normalized human attribute, and the population as a whole becomes respatialized as social constructions of space become morphed by networks.

Machine mediated space means that new and different boundaries are experienced based on the architecture of those machines. This is not to imply a dystopian science fiction plot, such as that of *The Matrix*, in which the human conscience only exists within digital bounds. The individual will certainly still exist and move through physical space, but there will be new understanding of the nature of boundaries and borders as individuals recognize an "extraordinary possibility for many to participate in the process of building and cultivating a culture that reaches far beyond local boundaries."[109]

As already noted, IoT is indicative of such networked space. IoT allows the networking of devices that can be controlled by electrical current, thus a small computer known as a microcontroller can be used to spin motors, adjust electrical current levels, flip switches, and accomplish a variety of other tasks. Microcontrollers with a network connection allow a user to exert control over physical space through a network connection.

One of the most popular applications of IoT is enabling home automation via the Internet, effectively networking an individual's physical personal space. Transaction points literally proliferate through the space of the home. For

instance, lights have traditionally been controlled with a physical switch implicitly requiring a person to move through the physical in order to operate it. IoT, though, ends the "who is turning off the lights" debate that so many couples have by removing the distance to the switch. More striking, it allows the user to turn the lights on or off from a foreign country and even allows an outside party to control the lights. The interior space once defined exclusively by the walls of a room is now open to new forms of control as those walls are breached. The borders physically defined by walls are no longer boundaries to certain types of computer mediated changes in that space. Needless to say this changes the experience and perception of the space of "home" for that user.

Notes

[1] "Static," *The Twilight Zone*, season 2, episode 20 (1961).

[2] *See, for example,* "A Thing About Machines," *The Twilight Zone*, season 1, episode 40 (1960).

[3] *For example*, Gompert & Saunders, *Paradox of Power* (2012) 115 ("Cyberspace [is] shorthand for the capabilities and content of computer networking."); Lessig, *Code 2.0* (2006) 9 ("But 'cyberspace' is something more. Though built on top of the Internet, cyberspace is a richer experience."); Toulouse, "Introduction" (1998) 5 (". . . a new transnational realm of civil society . . ."); Luke, "The Politics of Digital Inequality" (1998) 121 ("Cyberspace might best be understood as the latest manifestation of nature's pluralization."); and Betz & Stevens, *Cyberspace and the State* (2011) 13 ("Cyberspace is notoriously difficult to pin down.").

[4] Toulouse, "Introduction" (1998) 12.

[5] *For historical examples see*, Burbank & Cooper, *Empires in World History* (2010) 109–110; Mattelart, *Networking the World* (2000) 1–13; and Kellner, "Intellectuals, the New Public Sphere, and Technopolitics" (1998) 175–79.

[6] Cohen, "Privacy, Visibility, Transparency, and Exposure" (2008) 181.

[7] *Id.* at 190.

[8] *Id.* at 200.

[9] *See* Carey, "A Cultural Approach to Communication" (2002) 36–45.

[10] Lessig, *Code 2.0* (2004) 9 and Kulesza, *International Internet Law* (2013) 31.

[11] Goodman & Chen, "Modeling Policy for New Public Service Media Networks" (2010) 115.

[12] *See* Goodman & Chen, "Modelling Policy" (2010) 116; Werbach, "Breaking the Ice" (2005) 78–80 and Solum & Chung, "The Layers Principle" (2003) 821.

[13]Werbach, "Breaking the Ice" (2005) 71, 66.

[14] Gompert & Saunders, *Paradox of Power* (2012) 116. *See also* Leiner *et al*., "A Brief History of the Internet" (2012).

[15] Werbach, "Breaking the Ice" (2005) 66.

[16] Post, *Jefferson's Moose* (2012) 80–83.

[17] Kulesza, *International Internet Law* (2013) 125–126.

[18] Solum & Chung, "Layers Principle" (2003) 816.

[19] Werbach, “Breaking the Ice” (2005) 71.

[20] *Id.*; Werbach, “A Layered Model for Internet Policy” (2002) 37; Reed, “Critiquing the Layered Regulatory Model” (2005) 281; McTaggart, “A Layered Approach to Internet Legal Analysis” (2003) 573; and Lessig, *Code 2.0* (2004) 144–145.

[21] Werbach, “A Layered Model for Internet Policy” (2002) 60.

[22] Osgood, “Net Neutrality and the FCC Hack” (2004) 32.

[23] *Id.*

[24] Kende, “The Digital Handshake” (2000) 3.

[25] *See generally*, Krattenmaker, *Telecommunications Law and Policy* (1998) and Kennedy & Pastor, *An Introduction to International Telecommunications Law* (1996).

[26] Werbach, “Breaking the Ice” (2005) 61. *See also*, Kulesza, *International Internet Law* (2013) 53; McIntosh & Cates, “Hard Travelin’” (1998) 95, 102–03; Tambini, Leonardi, & Marsden, *Codifying Cyberspace* (2008) 3–4; Jayakar, “Globalization and the Legitimacy” (1998) 719.

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

[28] Werbach, “Breaking the Ice” (2005) 62; Post, “Against ‘Against Cyberanarchy’” (2002) 1375–76.

[29] *See* Post, *Jefferson’s Moose* (2012) chapters 4–6; Lessig, *Code 2.0* (2006) 43–45, and Clark & Landau, “Untangling Attribution,” (2010) 27.

[30] Brate, *Technomanifestos* (2002) 104–05.

[31] *See* DeNardis, *The Global War for Internet Governance* (2014) 37–41.

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

[33] *Id.*

[34] *Id.*

[35] *See* Post, *Jefferson’s Moose* (2012) 47–59.

[36] This is how the Internet was designed to operate, but it should be noted that deep packet inspection technologies are used by some entities. *See* DeNardis*, Global War* (2014) 206–07.

[37] Post, *Jefferson’s Moose* (2012) 80.

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

[39] Mattelart, *Networking the World* (2000) 4.

[40] *See* Betz & Stevens, *Cyberspace and the State* (2011) 38; Leiner *et al*., “A Brief History of the Internet” (2012)*;* and Fielder, “The Internet and Dissent in Authoritarian States” (2013) 168.

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

[42] *Id.*

[43] Lessig, *Code 2.0* (2006) 111.

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

[45] *See* Toulouse, "Introduction" (1998) 2 and Betz & Stevens, *Cyberspace and the State* (2011) 13.

[46] Leiner *et al*., "A Brief History of the Internet" (2012) *See also,* Verizon v. FCC, No. 11–1355, 740 F. 3d 623 (Court of Appeals, Dist. of Columbia Circuit 2014) at 36.

[47] The HTTP portion of the URL denotes the type of data being sought, in this case it stands for Hypertext Transfer Protocol. This portion of the address is a Uniform Resource Identifier (URI), and it identifies that a hypertext file is being sought. There are numerous URIs indicating the type of data a given application is seeking. These include the common File Transfer Protocol (FTP), Internet Chat Relay (IRC), and HTTP Secure (HTTPS).

[48] Partridge & Lonardo, "ICANN Can or Can It?" (2009) 24–29 and DeNardis, *Global War* (2014) 41–44.

[49] A server is an application on the applications layer. A server, though usually on specialized hardware, is simply a computer application that makes computer files available to other computers on a network. In this case the server has been configured to be open to requests from any network. Servers are essentially file systems configured in a hierarchical directory and can be understood to function in a substantially similar way to the file and folder system found in most desktop operating systems.

[50] Tambini *et al*, *Codifying Cyberspace* (2008)) 7. "index.html" is simply a filename and "index" is an arbitrary default filename for which browsers search as a result of their programming.

[51] Lessig, *Code 2.0* (2006) 268.

[52] Tambini *et al*, *Codifying Cyberspace* (2008) 2.

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

[54] *See* Tambini *et al*, *Codifying Cyberspace* (2008) 9; Leiner *et al*., "A Brief History of the Internet" (2012); and Goodman & Chen, "Modeling Policy" (2007) 120. *Compare with* Jayakar, "Globalization and the Legitimacy" (1998) 722; Krattenmaker, *Telecommunications Law and Policy* (1998) 367–69; and American Broadcasting Company v. Aereo, 573 U.S. __ (2014).

[55] Wakefield, "Smart LED Light Bulbs Leak Wi-Fi Passwords" (2014).

[56] Verizon v. FCC (2014) at 36.

[57] Greenberg, *This Machine Kills Secrets* (2012) 70–76.

[58] *Id.* at 72–74.

[59] International Traffic in Arms Regulations, 22 C.F.R. 121.1 Category XII(b) (2018).

[60] Thingiverse, https://www.thingiverse.com/ .

[61] *See generally* Eppenstein & Aisenberg, "Radio Propaganda in the Contexts of International Regulation and the Free Flow of Information as a Human Right" (1979) 54; Robertson, "The Suppression of Pirate Radio Broadcasting" (1982) 71–101; United Nations General Assembly, Res. 37/92: Principles Governing the Use by States of Artificial

Earth Satellites for International Direct Television Broadcasting" (1982); and EUTELSAT, "Eutelsat condemns jamming of broadcasts from Iran and renews appeals for decisive action to international regulators" (2012).

[62] Lessig, *Code 2.0* (2006) 9 and Kulesza, *International Internet Law* (2013) x–xi.

[63] Streck, "Pulling the Plug on Electronic Town Meetings" (1998) 20.

[64] *See generally* Post, *Jefferson's Moose* (2012) 68–69.

[65] International Telecommunications Union, *ICT Facts and Figures 2017* (2017) at 2.

[66] Goldsmith, "Against Cyberanarchy" (1998) 1201.

[67] Post, "Against 'Against Cyberanarchy'" (2002) 1374.

[68] *Id*.

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

[70] Brown, "Pirate Bay Mirror Is Proxy-Friendly, Bypasses UK Ban" (2012); Mlot, "The Pirate Bay Is Back Online (Sort Of)" (2014); and Hamill, "Pirate Bay Is BACK" (2015). *See also* Domscheit-Berg, *Inside WikiLeaks* (2011) 21.

[71] *But see* Gelernter, "The End of the Web Search and Computer as We Know it" (2013); Seife,*Decoding the Universe* (2007) and Lloyd, *Programming the Universe* (2006).

[72] Werbach, "Breaking the Ice" (2005) 79.

[73] Streck, "Pulling the Plug on Electronic Town Meetings" (1998) 26.

[74] Fritsch, "Technology and Global Affairs" (2011) 31.

[75] Streck, "Pulling the Plug on Electronic Town Meetings" (1998) 26.

[76] Lawrence Lessig, *Code 2.0* (2006) 9.

[77] Ferguson & Mansbach, *Globalization* (2012) 10.

[78] Barlow, "The Declaration of Independence for Cyberspace" (1996).

[79] Resnick, "Politics on the Internet" (1998) 51.

[80] Post, *Jefferson's Moose* (2012).

[81] Johnson & Post, "Law and Borders" (1996) 1379; *see also* Betz & Stevens, *Cyberspace and the State* (2011) 13.

[82] Gelernter, "The End" (2013) and Streck, "Pulling the Plug on Electronic Town Meetings" (1998) 26.

[83] *See* Lessig, *Code 2.0* (2006) 88–94.

[84] Heddaya, "See a Map, Not a Territory" (2013).

[85] Kulesza, *International Internet Law* (2013) xii.

[86] *For instance*, Johnson & Post, "Law and Borders" (1996) 1378.

[87] *Id*.

[88] *See* Kulesza, *International Internet Law* (2013) 29.

[89] Barlow, "A Declaration" (1996).

[90] Greenberg, *This Machine Kills Secrets* (2012) 256.

[91] Toulouse, "Introduction" (1998) 13.

[92] *See generally*, Merges, Menell, & Lemley, *Intellectual Property in the New Technological Age* (2012) 911–930.

[93] *See* Lessig, *Free Culture* (2004); Partridge & Lonardo, "ICANN Can or Can It?" (2009); and Ranieri, "EFFecting Digital Freedom" (2014) 52–53.

[94] Domscheit-Berg, *Inside WikiLeaks* (2011) 21.

[95] *See* Bearman, "The Untold Story" (2015).

[96] Spar, "The Public Face of Cyberspace" (1999) 348 and McIntosh & Cates, "Hard Travelin'" (1998) 95.

[97] *See* Tambini *et al*., *Codifying Cyberspace* (2008) 68 and Goodman, "Media Policy and Free Speech" (2007) 1221.

[98] Lessig, *Code 2.0* (2006) 298.

[99] Betz & Stevens, *Cyberspace and the State* (2011) 35.

[100] *For example compare*, *The Lawnmower Man* (New Line Cinema 1992) and *The Matrix* (Warner Brothers 1999).

[101] *See* Lessig, *Code 2.0* (2006) 108–111.

[102] Microsoft, "HoloLens" (2015).

[103] Stadtmiller, "Virtual Reality Sex Is Coming" (2015).

[104] Ramey, "When AT&T Asked Us to 'Reach out and Touch Someone', Did They Mean That Literally?" (2008).

[105] Oliver, "Stuxnet" (2013) 127–59.

[106] Post, *Jefferson's Moose* (2012) 31–36 and Lessig, *Code 2.0* (2006) 298.

[107] Luke, "The Politics of Digital Inequality" (1998) 123.

[108] e-Estonia, "What is e-Residency?" (2015).

[109] Lessig, *Free Culture* (2004) 9.

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.