THE LOGICS AND TERRITORIALITIES OF GEOBLOCKING

CAMERAN ASHRAF AND LUIS FELIPE ALVAREZ LEÓN

Introduction

The internet is often represented as an open network threatened by the aberrations of internet censorship and control. However, its historical development and architecture belie this binary model. The early split of the ARPANET by the U.S. Department of Defense into MILNET and ARPANET in order to protect sensitive military communications demonstrates that the ability to close and control the internet was by design part of its very foundation. Indeed, few states would embrace the internet were there not sufficient technical mechanisms to ensure an acceptable degree of management, surveillance, and control. In order to produce a better understanding of the political dimensions of the internet, the binary model of an open or closed system should be seen as part of a broader range of geopolitical and geoeconomic logics espoused by states and other actors, such as firms, who envision and construct the internet through different territorial perspectives.

The purpose of this chapter is to examine the territorialities associated with the internet through the lens of geoblocking. Geoblocking, from this perspective, is a phenomenon that brings together various actors, each with particular logics of action, and maps their corresponding territorialities onto the internet. The geopolitical and geoeconomic logics behind geoblocking and their resulting territorialities will be illustrated by a comparative examination of states and markets through two specific examples: state-sponsored internet censorship and online video distribution markets. These two perspectives reveal how geoblocking and its corresponding logics of deployment produce a range of territorialities that transcend the open/closed binary through which the internet is often understood.

States

The international state system is predicated upon geographical concepts which establish territorial states as distinct and discrete entities. The state is free to act within its territory, which is demarcated by borders, and its freedom to act within those borders is its sovereignty. Territory, borders, and sovereignty are the geographical assumptions underpinning the international state system. While these geographical concepts manifest themselves in many familiar ways, such as passport controls at airports or border fences, they need not be bound to the explicitly physical domain of land. Indeed, they have been adapted through airspace, territorial waters, and subterranean rights. The development of the internet, however, represents a new space for states to act and to reassert traditional notions of territory. For example, early cyber-utopians such as John Perry Barlow, co-founder of the Electronic Frontier Foundation, envisioned cyberspace as a radical space where borders and states no longer mattered: 'Governments of the Industrial World, you weary giants of flesh and

steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.'[1] In cyberspace one could be something radically different and no longer be constrained by any of the perceived drawbacks of the physical world, such as physical appearance or geography.

Contrary to this vision, states have engaged with cyberspace by adapting the ideas of territory, borders, and sovereignty to this environment through the development of internet censorship and control. This is a view of the internet as an extension of existing territory in the new informational space through the development of laws and technical systems to territorialize cyberspace. In effect, many aspects of the international state system became duplicated online, such that the internet experienced from within one state could radically differ from the internet experienced from another. Through utilizing internet controls states are able to restrict the flow of information inside and outside of their borders, regardless of political circumstances. In cyberspace internet filtering is the primary way states assert their geopolitical visions, which are founded on the principles of sovereignty and borders. This is the 'information curtain' first articulated by Secretary of State Hillary Clinton in 2010.[2]

The rise of state internet controls and internet filtering has led many scholars and critics to assert that the modern state has found renewed vigor and life online.[3] The libertarian and utopian visions surrounding the birth of cyberspace have given way to a colder realism whereby cyberspace as a prototypical global public sphere[4] or global cyber commons[5] is becoming increasingly balkanized and segmented geopolitically. Censorship implementation and circumvention are a major and growing industry, worth at least $1.2 billion dollars in 2012 and including well-known corporations such as Cisco Systems and McAfee.[6]

Activity Regulations

According to Jonathan Zittrain and John Palfrey, activity regulations embody the many levels in which state territorialities are mapped onto cyberspace. Rather than internet-specific laws, activity regulations often stem from extensions of pre-existing restrictions on freedom

1 John Perry Barlow, 'A Declaration of the Independence of Cyberspace', 8 February 1996, https://projects.eff.org/~barlow/Declaration-Final.html

2 Rebecca MacKinnon, 'China's "Networked Authoritarianism"', *Journal of Democracy* 22.2 (2011): 32-46.

3 Ronald Deibert, 'The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace', in Andrew Chadwick and Philip N. Howard (eds) *The Routledge Handbook of Internet Politics*, Abingdon: Routledge, 2009, pp. 323-336; Nart Villeneuve, 'The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace', *First Monday* 11.1 (2006); Jack Goldsmith and Tim Wu, *Who Controls the Internet?*, New York: Oxford University Press, 2008.

4 Zizi Papacharissi, 'The Virtual Sphere: The Internet as a Public Sphere', *New Media & Society* 4.1 (2002): 9-27.

5 Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge, Mass: The MIT Press, 2012. Choucri, *Cyberpolitics in International Relations*.

6 Orans and Firstbrook. 2011. 'Magic Quadrant for Secure Web Gateways.', Gartner Inc., available at https://www.gartner.com/doc/3064318/magic-quadrant-secure-web-gateways.

of speech or other media controls with the specific forms they take vary depending on social and political factors. For example, some states, such as Saudi Arabia or Iran, choose to enact content regulations to restrict or forbid citizens from developing, consuming, or distributing certain types of content. On the other hand, states may choose to 'relocate' content regulations by requiring internet service providers (ISPs) to filter content on behalf of the state in order to get a business license. Companies that do not filter on behalf of the state may be subject to various liabilities and penalties until they are in compliance. Finally, in states with pervasive surveillance regimes, users may engage in self-monitoring as a form of self-censorship echoing Foucault's panopticon whereby the user, company, ISP, or other user or provider censors themselves or the content and internet access they provide without prompting or intervention by the state. [7] This is often accompanied by a general level of surveillance and monitoring by the state that facilitates self-monitoring and surveillance as a social norm.

As with content classification, these filtering categories are not necessarily demarcated clearly, nor are their existence mutually exclusive. A state may implement some or all of these categories in their own interpretation of how best to protect and create informational sovereignty. In Iran, ISPs must obtain licenses, web hosting and mobile data plans require home addresses and personal registration, and cyber cafes must also register users while being under the threat of liability or licensing requirements.[8] In China the state includes its content restrictions in domestic copyright laws, creating a sheen of legitimacy and the appearance of working with international copyright norms while regulating content domestically. [9] Further, content restrictions may not be aimed solely at an individual user; a university or other organization may be held liable by a state for facilitating objectionable activities online as evidenced by the numerous copyright lawsuits filed by the Recording Industry Association of America (RIAA) against U.S. university students. While these activity regulations are often enforced to preserve state sovereignty, they can exist at the confluence of multiple logics. For example, the use of copyright by industry groups and enforced by the state can simultaneously advance a specific kind of market logic while also enacting state territoriality.

Technical Regulations

While activity regulations focus on *what* is controlled through the process of internet blocking, technical regulations focus on the instruments used to achieve this aim. Technical regulations and the technical specifics of internet filtering are expansive and vast. They can be grouped into four broad categories: in-line, DNS/domain tampering, denial of service, and national cyberzones.[10] Each category approaches filtering from a different perspective and each has

7 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, 2nd edition, New York: Vintage, 1995.

8 Jonathan Zittrain and John Gorham Palfrey, 'Internet Filtering: The Politics and Mechanisms of Control', in Ronald Deibert et al. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press, 2007, pp. 29-56.

9 Ibid.

10 Steven J. Murdoch and Ross Anderson, 'Tools and Technology of Internet Filtering', in Ronald Deibert et al. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press, 2008, pp. 57-72.

unique structural advantages and disadvantages. For example, in moments of political crisis the easiest method to intimidate and control information flows can be to attempt a denial of service attack either conventionally or through identifying weaknesses in an offending server/website and bringing it down.

In-line filtering is comprised of two methods: proxy filtering and TCP/IP filtering. Proxy filtering seeks to insert another server between the user and the internet. Users access this server, which retrieves content on behalf of the user. Doing so allows the proxy server to cache content, increasing performance and speed for the end user while allowing administrators to have detailed abilities to block specific assets rather than entire domains.[11] This approach limits the user's ability to connect directly to the internet, ensuring that virtually all content is localized within the territorial state, a technique used by Syria after the Arab Spring uprising.[12]

TCP/IP filtering is the most commonly known method of internet filtering. Data packets are inspected for specific attributes (IP address, domain name, service port number, etc.) and this is checked against a defined block list, usually provided by the state. This level of analysis can occur at a router level or require a deeper level of inspection. Filtering at the router level will examine just the header of the information packet – equivalent to the address on an envelope – and block or allow that packet to continue to its destination. Examining the content of the data packet – equivalent to opening the envelope and reading its contents – requires more sophisticated technologies, called Deep Packet Inspection (DPI), which is currently believed to be in use in Iran.[13]

In the DPI method of TCP/IP filtering, the data packets are checked not only at the header level, but the actual content of the packet is checked for prohibited content, search queries, words, or other information. These are then checked against another list automatically via algorithm, to determine whether the packet should continue to its destination or be dropped or blocked. Depending on the sophistication of the algorithm, the censor can capture or monitor a tremendous amount of information at a highly granular level. This system can be used to not only identify content, but to address specific signatures and patterns in encrypted communications and block those packets, as evidenced by the repeated blocking of the Tor circumvention and anonymity tool in Iran.[14]

Most websites and online content are accessed using domain names, such as Google.com or UCLA.edu. In order to effectively translate the human readable domain names into machine readable IP addresses, users must access their ISP's DNS server when requesting a website. This process is normally invisible to the user, but within a filtering regime the

11 Ibid.

12 T. Eissa and Gi-hwan Cho, 'Internet Anonymity in Syria, Challenges and Solution', in Kuinam J. Kim and Kyung-Yong Chung (eds), *IT Convergence and Security 2012*, Dordrecht: Springer Netherlands, 2012, pp. 177-86.

13 Simurgh Aryan, Homa Aryan, and J. Alex Halderman, 'Internet Censorship in Iran: A First Look', *Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet*, Washington, August 2013, https://jhalderm.com/pub/papers/iran-foci13.pdf.

14 Ibid.

ISP's DNS server is fed with a list of specific domain names that should be blocked. When a user attempts to access a website in a filtering regime with DNS tampering, they will be unable to see the page.

Domain modifications and tampering are the counterparts to DNS tampering. DNS tampering works to block a user within a national filtering regime from accessing specific content. However, users outside of the territorial filtering regime are still able to access that content. If, for example, a website located in the Sudan is reporting on atrocities within the country, then users in the home country would be unable to access the content, but international media, such as CNN or the BBC, would still be able to do so. Domain modifications prevent this by removing the DNS entry for the domain name from the national DNS servers, which outside users access in order to retrieve a domain.

The final category, denial of service, involves a range of actions undertaken by states to filter both domestically and internationally. It includes distributed denial of service (DDoS) attacks, hacking, surveillance, and content takedown. The central logic of the denial of service category is that it uses cyber-attacks and infiltration to remove or alter undesirable content, regardless of where it is located geographically.

Content takedowns are a relatively new method of filtering which reflects the explosion of user-generated content in the web. In this method, states and citizen sympathizers or paid actors 'flag' or report objectionable content to content providers in the hopes of having the offending content removed and the uploader banned.[15] If, for example, a protest video were uploaded to video sharing site YouTube, a content takedown would see state-affiliated actors register accounts and report the video to YouTube so that it would be removed automatically.

The previous examples impose the territoriality of states by actively filtering, blocking or removing content, thus altering information flows. Surveillance, on the other hand, employs social, political, legal, and technical means to observe, collect, and classify information from the general populace and other targets of interest to the state. In-line filtering, especially through DPI, aids in surveillance as all aspects of data packets can be examined and then routed for storage and further investigation. Surveillance supports filtering because it acts as a digital panopticon whereby users are uncertain if they are being observed or monitored, and thus practice self-censorship of content for fear of punishment or other sanction.[16] Thus, surveillance as a filtering method must be supported by social or legal consequences otherwise it lacks ability to facilitate filtering.

Finally, the creation of national cyberzones marks an approach where ‘hard’ territoriality that

15 Erica Newland et al., ‘Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users’, Berkman Center Research Publication, Harvard University, 2011, no. 2011-09.

16 Ronald Deibert, ‘Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace’, *Millennium-Journal of International Studies* 32.3 (2003): 501-30; Ronald Deibert and Rafal Rohozinski, ‘Liberation vs. Control: The Future of Cyberspace’, *Journal of Democracy* 21.4 (2010): 43-57.

mirrors the land boundaries of the state is deployed through internet controls[17] to fence in flows of information. This approach seeks to develop an internal or "national internet" whereby users can only access information located within their territorial borders by disconnecting from the broader internet and relying on an exclusively domestic one. International connections still exist, but are restricted to elites or those with other forms of government approval. North Korea's Kwangmyong network is the oldest example of a national cyberzone where users can only access websites and resources located within North Korea and approved by state information ministries.[18] As with many of the blocking techniques previously discussed, national cyberzones can also intersect state with market logic by creating market spaces that are free from external competition, thus producing conditions that favor specific (often state-backed) actors.

Geographical concepts such as borders, territory, and sovereignty thus have both technical and legal analogues that have supported and extended their conceptual development, mutation, and maturation throughout human history. The Treaty of Westphalia's principle of mutual recognition, for instance, was dependent upon surveying technologies that could accurately demarcate and communicate borders. Technology plays a critical role for states in demarcating their limits and extents as well as communicating and defending those extents. To achieve this, states must combine activity regulation within their geographies with demarcation of these geographies through technical regulation. In spite of ethereal metaphors such as 'the cloud', the internet is a tremendously territorial medium grounded in space with easily identifiable packets, standardized national domain registrars, transnational data agreements and configuration, and national or sub-national networks (autonomous systems) whose deployment is the foundation of the internet and the purview of states.[19]

Cyberspace is increasingly territorialized by states through activity and technical regulations. States see cyberspace as an extension of the existing geographical status quo and have extended their legal and technical domains to encompass this, while simultaneously beginning to pursue international conventions in cyberspace. However, states are not alone in mapping their territorialities onto cyberspace. Indeed, states often see markets and firms as integral to efforts to normalize territorialized cyberspace. Through the transactions of myriad actors, markets deploy their own specific territorialities onto information flows. While mostly guided by a profit-seeking logic, these territorialities are constantly in dialogue, interaction, and sometimes tension with those of the state. The following section discusses the guiding logics of markets and their associated territorialities on the internet, and in doing so demonstrates a non-state centric logic through which geoblocking produces a broad range of territorialities which transcend attempts to understand the internet through an open/closed binary perspective.

17 Ronald Deibert et al. (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, Mass: MIT Press, 2010.

18 Barney Warf, 'The Hermit Kingdom in Cyberspace: Unveiling the North Korean Internet', *Information, Communication & Society* 18.1 (2015): 109-20.

19 Hal Roberts, David Larochelle, Rob Faris, and John Palfrey. 2011. "Mapping Local Internet Control." In Computer Communications Workshop (Hyannis, CA, 2011), IEEE.

Markets

While states can control or record flows of information to preserve their sovereignty and territorial power online, market actors pursue a different type of territorialization: one that allows them to maximize profit. Often this involves 'locking information' through technical means, such as Digital Rights Management technologies, in order to target specific authorized spaces or devices. This means that the territorialities of information markets can be determined by the extent of market segmentation, distribution and enforcement of intellectual property rights, or the compatibility of technical means with particular digital goods.

In order to understand how market actors territorialize information, this process has to be put into the broader context of governance structures, such as regulatory frameworks. Intellectual property regimes, for example, have become instrumental in creating informational market spaces by limiting the distribution of content to specific jurisdictions. However, while this enables copyright holders, such as film studios, to secure revenue from distribution rights, it also presents new challenges. One of these is the difficulty of ensuring that only 'legitimate' content flows within the territorialized information markets. In digital environments it is very difficult to eradicate market-anomalous behavior such as piracy and file-sharing due to the low costs of reproduction and distribution online.

Another challenge for the construction of territorialized markets across digital information networks is the globalizing scale of information flows. This requires technical and governance frameworks such as payment systems and intellectual property protections to be coordinated across time and space at transnational scales. This level of coordination has made it more difficult to maintain a strategy long used by film distributors: the windowed release of products according to geographic region, and even by medium, such as theater and then home video. This strategy was designed to 'manage time and control speed through space so as to minimize the threat posed by new technologies'.[20] Consistent with the logic of market actors, the ultimate goal in this stepwise control of information is to reach the highest possible price each segmented market is capable of bearing.[21]

The distribution potential of digital networks presents a paradox to copyright holders and their efforts to map their particular territorialities onto these environments. While they present platforms for wider distribution and expanded markets, they also enable the development of actors who operate outside the bounds of those markets. Configured in fluid, decentralized assemblages such as P2P file-sharing networks and user communities, these actors often have the ability to circumvent the territorial and legal controls imposed by states and copyright holders.

20 Shujen Wang, 'Recontextualizing Copyright: Piracy, Hollywood, the State, and Globalization', *Cinema Journal* 43.1 (2003): 30.

21 Brett Christophers, 'The Territorial Fix: Price, Power and Profit in the Geographies of Markets', *Progress in Human Geography* 38.6 (2014): 754-770.

Operating beyond the bounds established by territorialized information markets, another type of information represents a potential for disruption to profit-maximization in markets. This is the spread of information outside the markets (through channels such as media outlets and social networks) *about* content circulating within those markets. The dissemination of this information may create network effects outside the markets that increase demand for content circulating inside them. Since digital goods such as films or TV shows are subject to the territorial limits of the market, but reviews, commentary and memes are not, this creates a spatial mismatch between the supply and demand. This means that some demand may not be satisfied by legal means outside of the markets due to either lack of authorized distribution or prices higher than most consumers will pay. As Shujen Wang points out, in the case of films and entertainment media, this has created an instant demand for pirated products.[22]

This tension between market territorialization and increased demand through digital networks *outside of the market* is an example of how new territorialities are extending old ones. While windowing the release of content by territory was an old strategy of copyright holders such as film studios, this is increasingly difficult in an era of global information flows. This has led to a multiplicity of coexisting strategies such as hard territorial markets through geoblocking, hybrid release campaigns across platforms, and simultaneous global releases.

Much like the controls of information enforced by states, the 'geographic rights management' approach behind geoblocking has been successful in producing territorialized spaces of information through exclusion. This process can be self-reinforcing because its deployment in a digital network environment expands the scope of its control with every digital copy. Lawrence Lessig has made the point that, through the use of DRM and the internet

> […] it is possible for [copyright holders] to centralize control over access to their content. Because each use of the Internet produces a copy, use on the Internet becomes subject of the copyright owner's control. The technology expands the scope of effective control because the technology builds a copy into every transaction.[23]

Yet, like states' control of information, which is often contested (and subverted) by groups of actors, the territorialities of information markets advanced by copyright holders are not permanently settled. In spite of the technical success of geoblocking technologies in territorializing content markets, copyright holders cannot permanently uphold their bid for control and centralization unless they offer audiences alternatives that meet their demands. This has forced copyright holders to seek different approaches that go beyond centralized control of information and punishment of violations.

As shown by the millions of takedown notices collected by the Chilling Effects project of the Berkman Center and the Electronic Frontier Foundation, it is common practice for copyright holders such as media companies, film studios, and states to demand the removal of

22 Shujen Wang, 'Recontextualizing Copyright', p. 31.
23 Lawrence Lessig, *Free Culture*, New York: The Penguin Press, 2004, p. 147.

copyrighted content from video streaming websites such as YouTube. However, while states seek to map their sovereignty and borders onto information networks, the profit-seeking logic of market actors is reflected in more malleable territorialities of information. For example, while the punishment of piracy was a key strategy to keep digital market spaces under control, copyright holders have opted to complement this approach with strategies aimed at capturing the lost revenue outside of the borders of these markets. Several studios have realized that if consumers are demanding video streaming online then the takedown notices and restrictions on streaming sites should be coupled with legitimate supply alternatives that address such unmet demand. That is how the service Hulu was born in 2008, which offers free streaming audiovisual copyrighted content available anytime with reduced commercial breaks. In a similar fashion, the television network websites are now offering part of their media catalogs in streaming content free of charge.

These alternatives are premised on the capacity of the copyright holders and distributors to enforce access controls on a territorial basis. These video platforms are offered within the bounds of states or regions that can provide a legal framework, a technological infrastructure, and a target audience receptive to the media products they offer and the advertisements that accompany them. Hulu, for example, detects if the IP number – which identifies the physical location of a computer – is within the United States or Japan, the two markets where this service operates. While for some time users abroad were able to circumvent these controls through the use of Virtual Private Networks or other technologies[24], Hulu has now blocked this possibility[25] – further demonstrating the territorialized construction of their market.

These video platforms present building blocks in territorialized information markets that have the dual aim of restricting access to a specific territory for legal purposes and also of providing highly differentiated marketing opportunities for their sponsors at a local level. Since markets cannot be created only through exclusion, but require the negotiation of supply and demand, this means that content is not only restricted through geoblocking, but also tailored by the information provided by geo-targeting and geographic rights management systems. This process of delimiting an audience geographically and constructing territorial information markets is a step towards creating “a well-mannered marketplace”, the fabled walled garden of the internet.

Geoblocking and DRM are technical means used by market actors to achieve territorialities that can maximize their profit. These territorialities do not substitute existing political geographies, such as state borders, but complement and often correlate with them. As was argued above, the territorialities of information markets necessitate the regulatory protection that can be offered by confining the dissemination of (supposedly borderless) information to the physical boundaries of particular jurisdictions. This of course allows for the application of jurisdiction-specific copyright laws jointly with the deployment of Digital Rights Management,

24 Hulu, ‘Why Can't I Use Hulu Internationally?', n.d., http://www.hulu.com/help/articles/171122.

25 Jeff Stone, ‘Hulu Streaming: How To Evade The Ban On VPNs And Continue Watching Online TV’,*IB Times,* 7 July 2014, http://www.ibtimes.com/hulu-streaming-how-evade-ban-vpns-continue-watching-online-tv-1620940.

which would be much more difficult to oversee in users and markets in other locations.

The complexities of enforcement highlight the continued presence of state institutional frameworks on the internet and the intersections between the territorialities of states and market actors in this environment. An example that illustrates this intersection is the recent Megaupload case, where millionaire Kim Dotcom was apprehended in New Zealand in 2012 at the behest of US authorities for illegally hosting copyrighted content in his storage service. In this case the reason why the United States Department of Justice could claim jurisdiction was due to the location of Megaupload's hired servers in Virginia. This confluence of factors resulting in a claim of territorial jurisdiction and extraterritorial prosecution is, however (for now), an exceptional case. Needless to say, much extra-legal copyrighted content distribution takes place outside of the bounds of jurisdictions actively protected by legal regimes and law enforcement agencies.

In an age of intense global competition the territorialities of online markets are increasingly important for copyright industries. Market segmentation strategies with rigid territorialities that rely on windowed releases are becoming increasingly difficult in light of the fluidity and reach of digital networks. These technologies have the potential to bring new competitors and enable current market leaders to deploy a multiplicity of territorial strategies. While the infrastructural advantages of Hollywood studios and Anglo-European media conglomerates are undeniable, the competition from emerging competitors such as Korean and Chinese media industries highlights the imperative to adapt in order to survive. The American film production system successfully navigated a structural reconfiguration in the middle of the 20th century, when its transformation from a vertically integrated industry to a network dominated by flexible specialization ensured its survival.[26] However, the challenge copyright holders face today is unprecedented in the sense that it entails a fundamental reconfiguration of media markets through the coexistence of multiple and shifting territorialities.

If new and established copyright holders aim to develop markets internationally, they must do so increasingly through digital networks. The successful construction and profitable operation of digital markets requires a balancing act between two countervailing forces. On the one hand, copyright holders enact territorialities through enforcement and control (by combining technical and legal means, such as geoblocking and copyright law). On the other hand, (legal and illegal) competition forces them to negotiate unmet market demand by developing alternative territorialities through new forms of distribution. These territorialities are built on the logic of profit-seeking, but also intersect with technical capabilities and politico-legal frameworks necessary to establish functioning markets. Thus, a key challenge in this project is the construction of stable territorialities of information markets. This requires considerable maneuvering and negotiation between judicial systems, technology firms, content providers, business strategies and consumer demands.

26 Allen J. Scott, *On Hollywood: The Place, The Industry*, Princeton: Princeton University Press, 2005.

Conclusion

Different actors have different territorial logics through which the internet is envisioned and created. Certain actors, such as states and firms, articulate clear territorialities based on intellectual property regimes, markets, and internet censorship or control. The existence of an "open" internet can be considered a techno-utopian vision at odds with the historical development of this network.[27] Indeed, the word 'geoblocking' presupposes that there is something to be blocked, necessitating a binary open/closed model of the internet. This idea represents yet another frame of territorial logic mapped onto the internet. However, as this chapter demonstrates, multiple actors envision the internet less as an open network and more structured around territorialized logics in pursuit of their own economic, political, and social goals. Thus, the internet as a medium of experience is heterogeneous rather than binary with multiple actors co-existing with and creating multiple internets. This is the internet of lived experience rather than one which is only conceptual or rhetorical: an internet whose terrain is as varied as the globe it spans.

References

Aryan, Simurgh, Homa Aryan, and J. Alex Halderman. 'Internet Censorship in Iran: A First Look', *Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet,* Washington, August 2013, https://jhalderm.com/pub/papers/iran-foci13.pdf.

Bendrath, Ralf, Johan Eriksson, and Giampiero Giacomello. 'From "Cyberterrorism" to "Cyberwar", Back and Forth', in Johan Eriksson and Giampiero Giacomello (eds), *International Relations and Security in the Digital Age*, Abingdon: Routledge, 2007, pp. 57-82.

Barlow, John Perry. 'A Declaration of the Independence of Cyberspace,' 8 February 1996, https://homes.eff.org/~barlow/Declaration-Final.html.

Choucri, Nazli. *Cyberpolitics in International Relations*, Cambridge, Mass: The MIT Press, 2012.

Christophers, Brett. 'The Territorial Fix: Price, Power and Profit in the Geographies of Markets', *Progress in Human Geography* 38.6 (2014): 1-17.

Deibert, Ronald. 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millennium-Journal of International Studies* 32.3 (2003): 501-30.

Deibert, Ronald. 'The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace', in Andrew Chadwick and Philip N. Howard (eds) *The Routledge Handbook of Internet Politics*, Abingdon: Routledge, 2009, pp. 323-336.

Deibert, Ronald et al. *Access Controlled: The Shaping of Power, Rights,and Rule in Cyberspace*. Cambridge, Mass: MIT Press, 2010.

Deibert, Ronald, and Rafal Rohozinski. 'Liberation vs. Control: The Future of Cyberspace', *Journal of Democracy* 21.4 (2010): 43-57.

Digital Element, 'Geographic Rights Management', http://www.digital-element.net/our_technology/our_technology.html.

Eissa, T., and Gi-hwan Cho. 'Internet Anonymity in Syria, Challenges and Solution', in Kuinam J. Kim and Kyung-Yong Chung (eds), *IT Convergence and Security 2012*, Dordrecht: Springer Netherlands,

27 Roberts, Hal, David Larochelle, Rob Faris, and John Palfrey. 2011. 'Mapping Local Internet Control.' In Computer Communications Workshop (Hyannis, CA, 2011), IEEE

2012, pp. 177-86.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, 2nd edition, New York: Vintage, 1995.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet?: Illusions of a Borderless World*, New York: Oxford University Press, 2008.

Hulu, 'Why Can't I Use Hulu Internationally?', n.d., http://www.hulu.com/help/articles/171122.

Lessig, Lawrence. *Free Culture*, New York: Penguin, 2004.

MacKinnon, Rebecca. 'China's "Networked Authoritarianism"' *Journal of Democracy* 22.2 (2011): 32-46.

Murdoch, Steven J., and Ross Anderson. 'Tools and Technology of Internet Filtering', in Ronald Deibert et al. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press, 2008, pp. 57-72.

Newland, Erica et al. 2011. 'Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users', *Berkman Center Research Publication*, Harvard University, no. 2011-09.

Orans, L., and P. Firstbrook. 2011. 'Magic Quadrant for Secure Web Gateways.' *Gartner Inc.*, http://www.gartner.com/technology/research/methodologies/magicQuadrants.jsp.

Papacharissi, Zizi. 'The Virtual Sphere: The Internet as a Public Sphere', *New Media & Society* 4.1 (2002): 9-27.

Roberts, Hal, David Larochelle, Rob Faris, and John Palfrey. 2011. "Mapping Local Internet Control." In Computer Communications Workshop (Hyannis, CA, 2011), IEEE.

Scott, Allen J. *On Hollywood: The Place, The Industry*. Princeton: Princeton University Press, 2005.

Stone, Jeff, 'Hulu Streaming: How To Evade The Ban On VPNs And Continue Watching Online TV', *IB Times*, 7 July 2014, http://www.ibtimes.com/hulu-streaming-how-evade-ban-vpns-continue-watching-online-tv-1620940.

Stryszowski, Piotr and Danny Scorpecci. *Piracy of Digital Content*,Paris: OECD, 2009.

Thomas, Julie. 'Ethics of Hacktivism.' *Information Security Reading Room* 12 (2001).

Villeneuve, Nart. 'The Filtering Matrix: Integrated Mechanisms of Information Control and the Demarcation of Borders in Cyberspace', *First Monday* 11.1 (2006), http://firstmonday.org/ojs/index.php/fm/article/view/1307/1227.

Wang, Shujen. 'Recontextualizing Copyright: Piracy, Hollywood, the State, and Globalization', *Cinema Journal* 43.1 (2003): 25-43.

Warf, Barney. 'The Hermit Kingdom in Cyberspace: Unveiling the North Korean Internet', *Information, Communication & Society* 18.1 (2015):109-20.

Zittrain, Jonathan, and John Gorham Palfrey. 'Internet Filtering: The Politics and Mechanisms of Control', in Ronald Deibert et al. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press, 2007, pp. 29-56.