INTRODUCTION: THE NEW VIDEO GEOGRAPHY

RAMON LOBATO

This book is about the cultural geography of video streaming. It is about platforms – YouTube, iPlayer, DailyMotion, Netflix, Periscope, Youku – and how they manage their international audiences and shape them into markets. It is about governments, state institutions and public-service broadcasters, and the technologies they use to regulate video flows across national borders. It is about users and audiences, and how they negotiate diverse forms of access and restriction. Above all, it is about cultural circulation – how different kinds of content reach dispersed audiences through authorized and unauthorized channels.

As an entry point into these wider issues, contributors to this book focus on a specific technology of access control: geoblocking. Geoblocking, a spatially-aware filtering technology that uses IP address databases to determine a user's location, has become a key mechanism for managing international video streaming traffic and maintaining separation of national media markets. The process is simple: when you visit a website, your IP address (e.g. 198.8.80.200) is run through a database to identify your ISP and geographic location, which is then matched against a blacklist or whitelist to establish access rights. If you are in an approved location, access is granted and the video automatically plays. Those outside the authorized zone will likely see a familiar error message – something like 'this video is not available in your region' – or perhaps an endlessly buffering screen.

Most major video platforms use geoblocking to filter international audiences. Geoblocking allows these platforms to customise their offerings according to territory, language, and advertising markets, and provides an automated mechanism to enforce territorial licensing arrangements with rights-holders. In this sense it is a form of access control enacted at the level of content and platform regulation, rather than network infrastructure.[1] But geoblocking has more subtle effects as well. Like search localisation and algorithmic recommendation, geoblocking is a 'soft' form of cultural regulation. Its widespread adoption is changing the nature of the open internet by locating users within national cyberspaces and customising content based on certain ideas about territorial markets.

Geoblocking and Global Video Culture takes these issues as the basis for a critical and eclectic discussion of the internet's changing cultural geography. Many contributors to this book are screen scholars, interested in the politics of media globalisation and how this translates into the digital environment. Other contributors approach the topic through legal analysis, cultural history, and spatial theory. Together, these essays offer a series of distinctive stories about a fast-changing and complex issue. Mixing macro-level insights with bottom-up accounts of everyday user experience, and moving from Europe to South

1 In this sense our approach can be distinguished from studies of the material infrastructure of the internet. For example, see: Lisa Parks and Nicole Starosielski, *Signal Traffic: Critical Studies of Media Infrastructures*, University of Illinois Press, 2015.

America to the Asia-Pacific, the various essays in this book provide provocative arguments about the cultural implications of the new video geography.

A major theme of the book is circumvention. As with many digital rights management technologies, geoblocking systems can be easily tricked. In recent years the appearance of user-friendly circumvention tools – including VPNs (virtual private networks), DNS (domain name system) proxies, web proxies, and location-masking browser extensions – has unleashed a wave of unauthorised cross-border media activity, allowing audiences to easily access streaming, news and sports services from other countries. As we shall soon see, these and other tools are used by a wide cross-section of users, and for remarkably different purposes. In exploring these various forms of blockage and circumvention, and the connections between them, our aim is to tell a different kind of story about internet blocking beyond the 'digital divide' paradigm.

Geoblocking circumvention is closely linked to other issues including internet governance, censorship, and cultural policy, because the same privacy tools that can be used to hack into iPlayer or Hulu are in other contexts used to get around state internet censorship. As researchers at Harvard University's Berkman Center for Internet and Society have documented, global circumvention – encompassing the use of commercial VPNs, activist-designed tools, simple web proxies and HTTP/SOCKS proxies – is an activity that involves tens of millions of internet users worldwide.[2] In Turkey, Iran, China and other nations where popular video and social networking platforms are regularly blocked by the state, circumvention is a mainstream practice.

One of our aims in *Geoblocking and Global Video Culture* is to explore linkages between these various blocking and circumvention practices – site-blocking, geoblocking, and the tactics people use to get around them. To this end, we have organized the book into two sections. The first section, 'Perspectives on Geoblocking', probes the historical, legal and cultural dimensions of geo-location and region control in media industries. These essays investigate a diverse array of platforms – from live-streaming apps and illegal streaming websites to the game consoles of the 1980s – and provide theoretical tools to understand the evolution of regional lock-out technologies in particular media sectors. The second section, 'Circumvention Case Studies', looks at these issues from the ground up, by analysing how users negotiate geoblocking and internet filtering controls in different countries. Here, our nine contributors – experts on informal media circulation that we have collaborated with over the course of a year-long research project – have written vivid first-hand accounts of ground-level circumvention practices in nine countries: China, Australia, Turkey, Sweden, Malaysia, Brazil, Iran, Cuba and the United States. Each of these countries has a different

2 Berkman Center researchers have produced a series of pioneering studies of internet filtering, censorship and circumvention. See: Ronald Deibert et al. (eds), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press, 2008; Hal Roberts et al, *2010 Circumvention Tool Usage Report*, Cambridge, MA: Berkman Center for Internet and Society, 2010; Deibert et al (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, MA: MIT Press, 2010; Deibert et al. (eds), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, Cambridge, MA; MIT Press, 2012.

story to tell when it comes to geoblocking, and together these accounts provide a fascinating snapshot of global circumvention practice (broadly defined).

To provide a taste of what is to come, I will now introduce three cross-cutting issues that connect the various essays in this book. First, I discuss the experience of blockage as a foundational logic of the internet; second, the history of circumvention technologies and practices; and third, the relationship between political censorship and pleasurable consumption, as seen through the lens of geoblocking.

Blockage and Flow

One of our starting points when developing the idea for this book was the uncontroversial observation that, for many internet users, the experience of online video is characterised by blockage rather than flow. Governments (and ISPs) block internet sites for reasons related to public policy and political expediency. Media companies use geo-filtering to screen out undesirable audiences. Poor infrastructure and choked servers lead to delays, dropouts and buffering. The end result of these back-end blockages, from the perspective of the end-user, is that digital video culture becomes a set of unevenly distributed experiences with a peculiar geography of availability and unavailability. As Ira Wagman and Peter Urquhart observe, 'the fact remains that *where* you access the internet says a lot about *what kind* of internet you experience'.[3]

This is the messy reality of today's digital video ecology. Rather than free flow and instant access, the actually-existing experience from the user's perspective typically involves a series of partially-available platforms that shift and change according to one's location – a lumpy landscape of formal and informal services that sometimes work and sometimes do not, depending on where you are located. Consider the following examples:

- YouTube is available in 70 different country-specific versions, including dedicated platforms for countries such as Latvia and Yemen. But it is blocked in China, Iran, Pakistan and Syria, among other countries, and is intermittently unavailable in Thailand, Turkey, Bangladesh and Morocco.

- YouTube also has significantly restricted content in Germany because of a long-running copyright dispute with music collecting societies.

- The Netflix streaming catalog (as of 2016, unblocked everywhere but China) varies markedly between countries, with the availability of movies and TV content reflecting local licensing, copyright and censorship arrangements.

- Major streaming sites including BBC iPlayer and Hulu are available only in their coun-

3 Ira Wagman and Peter Urquhart, '"This content is not available in your region": Geoblocking culture in Canada', in Darren Wershle, Rosemary Coombe and Martin Zeilinger (eds), *Dynamic Fair Dealing: Creating Canadian Culture Online*, Toronto: University of Toronto Press, 2014, pp. 126.

try of origin (the United Kingdom and United States, respectively) and are geoblocked everywhere else.

- The catalogues of 'global' services such as Google Play, Amazon and iTunes vary widely between countries in terms of the content they offer and how much they charge for it, with 40%-50% price differentials between countries being a common occurrence.

- Wealthy countries have abundant local catch-up TV while poorer countries have little or none, and rely on piracy as a post-broadcast circulatory system.

As this list suggests, video services are fast and free in some countries but are unavailable or prohibitively expensive in others. These examples underscore the enduring importance of geography to digital video culture, reminding us that where we live – or at least where websites think we live – makes a big difference to how we experience the digital.

Jack Goldsmith and Tim Wu argue that internet history since the late 1990s can be described as a process of 'becoming bordered'. 'The result,' they write, 'is an internet that differs among nations and regions that are increasingly separated by walls of bandwidth, language, and filters'.[4] The end result is the fragmentation of the internet into a series of localised experiences and filtered environments. We are not just talking here about the infrastructural geography of networks, according to which some countries and demographics are blessed with cheap and fast connectivity while others live with dial-up, mobile-only, or no access at all. Instead, we are referring to an overlapping political-economic geography of content and service availability, shaped by market forces, licensing arrangements and state control, and which is premised on the availability of geo-location databases, geo-caching services (offered by content delivery networks such as Akamai), and location-aware credit card processing.

Geolocation technology dates back to the end of the 1990s when the first tech companies specialising in location detection, such as Infosplit, began to appear. Up to this point, most websites had only one interface for all global users. The more sophisticated corporate sites would customise their offerings based on user-entered information (*Please select your country/region*). But with the rise of geolocation databases and third-party location-detection services, it became practical to automate this process. Now location could be determined by IP address, with pages detecting your location then loading language- and territory-specific content to suit. The accuracy of these IP geolocation systems was sometimes questionable, as many readers will no doubt remember, and the present system still involves a messy patchwork of different databases that do not always play well together. But over time the kinks have been gradually ironed out to a point where IP geolocation works as intended most of the time.

4 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press, 2006, p. viii.

To the delight of digital advertising companies, content could now be customised to local markets. Websites could now imagine, understand and process their customers in geographic market segments, down to their postcodes (Hulu, for example, boasts it 'can target [ads] by Nielsen DMA, State or zip code')[5]. For internet idealists with their dreams of global connectivity and universal access, this resurgence of physical geography has been problematic. One widely discussed consequence is that there is now no such thing as a universal internet – understood as a stable set of globally available cultural materials – because customisation means that content and experience change according to location.

This brings us to television, and to its ongoing metamorphosis into an online medium. As television becomes a streaming service, delivered over the internet rather than through the airwaves, it becomes location-aware (and location-blind) in new ways. IP geolocation now serves a primary role in determining what content is available where, reconfiguring the spatial 'footprints' and access-control functions familiar to us from the broadcast model (TV as a local/national medium transmitted over the airwaves) and through direct-broadcast satellite transmission (TV as a set of internationally available but locally decoded channels).[6] In other words, geoblocking becomes a kind of de facto global cultural policy, shaping the communication environment by making available certain kinds of materials, while restricting others.

One implication of this new TV landscape is that internet theory and broadcast history are brought closer together. Approaching the internet as a localised and unevenly available set of cultural experiences – as opposed to a global, universal superhighway – reminds us that the internet, like television, is always locally configured as well as globally networked. This diversity of institutional forms is noted by global television scholars, who emphasise that TV production cultures, advertising systems, and regulatory frameworks still vary significantly between countries. As Graeme Turner and Jinna Tay write in *Television Studies after TV*, 'Notwithstanding the internationalization of the media industries, these days the answer to the question 'What is television?' very much depends on where you are'.[7] Turner and Tay didn't have geoblocking in mind when they wrote that sentence, but they may as well have. Geoblocking reminds us that geography matters a great deal to television, and never moreso than in the internet age.

Control and Circumvention

A second cross-cutting theme in our book is circumvention – the tactics, tools and workarounds that people use to access blocked video sites. As our contributors elegantly describe, the geography of blockage and flow is provisional rather than absolute because

5 Derek Kompare, 'Adverstreaming: Hulu Plus', *Flow*, 24 Feb 2014, http://flowtv.org/2014/02/adverstreaming-hulu-plus/.

6 These issues have been explored through key works in video geography, to which we are indebted. See: Tom O'Regan, 'From Piracy to Sovereignty: International VCR Trends', *Continuum: The Australian Journal of Media & Culture*, 4.2 (1991): 112-135; Brett Christophers, *Envisioning Media Power: On Capital and Geographies of Television* Lanham: Lexington Books, 2009.

7 Graeme Turner and Jinna Tay, *Television Studies after TV: Understanding Television in the Post-Broadcast Era*, London: Routledge, 2009, p.8.

internet users have many ways to work around geographic restrictions. Indeed, IP address geoblocking is particularly easy to circumvent through basic software tools – including VPNs, DNS proxies, web proxies, and TOR – which can unlock geo-restricted content by rerouting data through an offshore IP address, making it appear as though the user is located in another country. In recent years a growing ecology of circumvention tools has emerged, including free ad-supported services (Hotspot Shield, Hola, Addtelly), subscription VPNs (Private internet Access, HotSpotNordVPN, TigerVPN), and DNS proxies designed explicitly for unlocking offshore content (Unblock-US, Getflix).

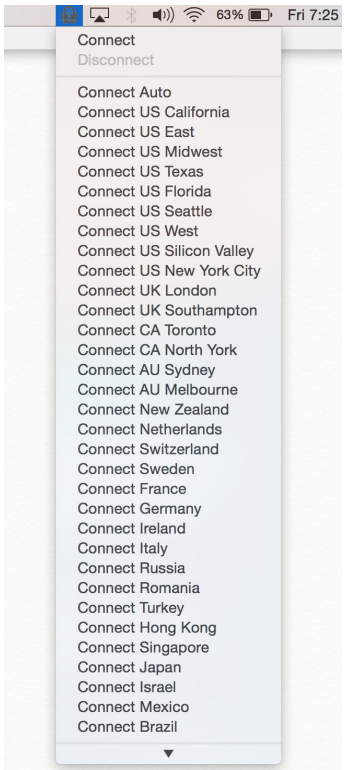

Figure 1. A VPN server selection menu

Figure 1b. A Twitter exchange following Netflix's global expansion on 6 January 2016

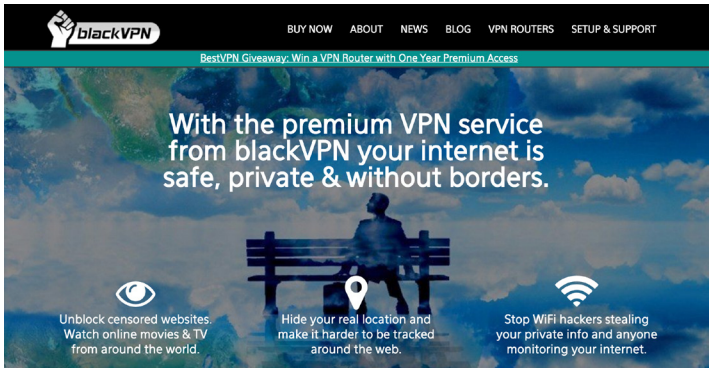

Figure 2. VPN marketing highlights unblocking functions

Circumvention is a complex topic, because most technologies used for geoblocking circumvention were not designed for this purpose and have other, licit functions. For example, VPNs are a popular security tool with privacy-conscious internet users who want extra protection when using public wifi networks. Others use VPNs for business-related networking or to dial into remote servers when working from home. There is nothing questionable about these activities, which are increasingly part of mainstream computer use. Indeed, many consumer groups advocate VPN adoption as a protection measure against hacking and identity theft. But VPNs are confounding objects for internet governance because they erode the link between IP address, location and identity. Allowing users to 'tunnel' outside national borders, they offer an ideal workaround for geoblocking, filtering and site-blocking, while presenting complex challenges for governments and media corporations.

Our point here is that there are different kinds of circumvention and proxying practices, associated with different kinds of internet use, and enabled by different kinds of software tools – and none of these things can be conflated in a straightforward manner. As Roberts, Zuckerman and Palfrey write, circumvention needs to be understood as 'a large topic that reaches deeply into a number of other large topics, including filtering, privacy, surveillance, and content neutrality'.[8] While the focus of this book is on geoblocking circumvention, many contributors in Section Two of the book also look at site-blocking circumvention, anonymization, and the links between these practices.

In China, Iran and Turkey, for example, circumvention tools are used widely because they open up access to YouTube, Twitter, and other blocked sites. Some of this activity is politically inflected but a lot of it is simply about social networking. In Australia, Sweden, and Brazil, in contrast, circumvention is more about access to first-release movies and TV, and to the expanded streaming catalogues available in the major markets. Some countries, such as Malaysia, display a mix of these two tendencies. In all cases, circumvention interfaces with anonymization and privacy, but not always in predictable ways.

8 Hal Roberts, Ethan Zuckerman, and John Palfrey, *2007 Circumvention Landscape Report: Methods, Uses, and Tools,* Cambridge, MA: The Berkman Center for Internet and Society, Harvard University, 2007, p. 9.

Thinking about circumvention from this perspective makes visible an array of everyday location-masking practices, from prosaic acts of access (Chinese teenagers using proxies to log into Facebook and YouTube, German tourists streaming Euro league matches) through to more overtly political resistances (as when Turkish activists share proxy settings in defiance of government internet censorship). So there is a nexus here between corporate media policies, censorship and circumvention, which are all linked through the use of informal software hacks. As our contributors show, this nexus is a rich site for theorising. In the small-scale tactics of internet circumvention we see larger stories unfolding about cultural regulation, networked activism, and cyber-identity.

There are also interesting possibilities here for media historiography, and for understanding the social shaping of network technologies. Each piece of circumvention software has its own fascinating and largely untold history: the VPN, for example, has been around for decades and was used primarily as a business networking tool until the early 2000s when it morphed into a personal computing product. Since then hundreds of small VPN companies have appeared and disappeared (by our count, there are at least 140 VPN brands in the market). In addition to these international VPNs, there are also 'local' VPNs running in some countries, notably Iran, which have Persian-language interfaces and local payment systems. There is much scepticism as to the bona fides of these companies, which are seen to be government-linked, but people use them anyway because they are functional and cheap. In this unusual state-supervised circumvention practice we see a strange mix of sanctioned and unauthorised, formal and informal, all blurring together.

Some popular VPNs, such as the British service Hide My Ass, have become major commercial enterprises. Founded in 2005 by a sixteen year old high-school student from Norfolk, Jack Cator, Hide My Ass has built itself into a mainstream privacy brand. Between its current VPN offering and its older web proxy service – which was tailor-made for kids to get around social media blocks on school computers – Hide My Ass claims to have had more than two million customers over the years, with 200,000 paying subscribers currently on the books, and almost 100 staff based in London, Kiev and Belgrade. This growth has paid off handsomely for Cator, who in 2015 cashed in and sold his business to the antivirus company AVG for £40 million.[9]

Browser plug-ins such as Unotelly and Hola Unblocker are another popular circumvention option. These proxy services are even easier to use than VPNs: just select a country or platform in the browser menu bar, and your IP address will be changed accordingly. Unlike VPNs, these are free services that do not require signup or subscription. But there is sometimes a hidden cost: the possibility for your IP address to be hijacked, as Hola users recently discovered when their bandwidth was loaned out to a third-party company for a botnet attack.[10]

9 Peter Shadbolt, 'How Misbehaving at School Made One Man a Millionaire', *BBC News*, 18 May 2015, http://www.bbc.com/news/business-32702501.

10 Ian Paul, 'Ultra-popular Hola VPN Extension Sold Your Bandwidth for use in a Botnet Attack', *PC World*, 29 May 2015, http://www.pcworld.com/article/2928340/ultra-popular-hola-vpn-extension-sold-your-bandwidth-for-use-in-a-botnet-attack.html.

Experiences such as this are common when it comes to free or ad-supported circumvention tools, especially apps, browsers extensions and web proxies with questionable business models that aren't immediately apparent to the end user. The number of free tools is always on the rise but the landscape is cluttered with commercial options of varying legitimacy and security, and the risk of virus and malware infection is ever-present.

Alongside these commercial products, there are other kinds of circumvention tools designed explicitly to get around government censorship. The peer-to-peer proxy service Lantern, for example, provides a popular way to evade national internet filtering. Lantern works by linking together users in filtered countries with a trusted international network of volunteers who share access to their IP addresses. A mix of start-up, NGO and private company, Lantern is ostensibly non-profit but somewhat opaque in its ambitions. It has been funded by the US State Department, reflecting the wider interest in circumvention technologies as tools of foreign policy.

As these examples suggest, internet circumvention is a space that brings together a strange mix of actors: activists, governments, entrepreneurs, criminals, geeks, pirates, school kids, and millions of ordinary people who wish to be conceal their identity or location temporarily. The chapters in this book trace out some of these unlikely connections in rich detail.

Censorship and Consumption

A third theme in this book is the relationship between market and state – or more specifically, the relationship between commercial technologies of access control and government site-blocking, surveillance and censorship. As we have seen already, from the user's perspective these two realities are closely intertwined: the geography of digital markets is overlaid with a political geography of unavailability. While technologically distinct, these two control systems need to be considered in tandem if we are to understand their cultural ramifications.

Geoblocking and government site-blocking occupy different ideological terrain. Geoblocking is typically discussed as an issue of access to markets and services. The paradigm here is consumer rights, rather than communication or citizenship. Key voices in the debate include early adopters, TV buffs and groups like the Electronic Frontier Foundation, all strident critics of geoblocking. In contrast, discussion of site-blocking tends to occur within a paradigm of internet freedom, and is typically linked to a discourse of free speech, political liberalism, communication rights and cyber-liberties.

Internet freedom is based on the idea that digital communication is inherently liberating and access control is inherently suspect. It tends to see the world through an ontology of free and unfree countries. A shortcoming of the internet freedom literature is that it has little to say about the everyday politics of pleasure and consumption. This realm, so familiar to media and culture critics, has been absent from the debate about internet filtering and censorship, which takes as its prototypical text not the quotidian experience of checking Facebook or watching a movie but the exceptional experience of political agitation, activism and resis-

tance. Our book tries very deliberately to work across this gulf, foregrounding traces of the political in the everyday and vice versa. As the following chapters demonstrate, there is no clear distinction between pleasure and politics in internet use.

Does a Chinese VPN user need to be accessing an anti-government news site for their activities to be considered 'political'? If they are just accessing Facebook to catch up with friends, does that matter? Conversely, what larger political issues surround the seemingly innocuous acts of everyday consumption enabled by entertainment-related circumvention in the ostensibly 'free' West? What temporary political affiliations and alliances may be produced in the consumer VPN scene? These are some of the questions that arise when we think about consumption and censorship together.

Rather than distinguishing between free and unfree societies, we take as our departure point the understanding that internet access and cultural consumption in all nations are shaped by overlapping forms of power, including both state and market power. We keep an open mind to some of the larger ethical questions lurking behind the internet freedom debates, such as whether access in its own right is always unequivocally a good thing, and whether states have the right to regulate their national internet space.

We also pay attention to how ideas of internet censorship and consumption are articulated, valued and debated according to cultural context. As contributors to this book show, the problem of geoblocking plays out quite differently in different countries. With the possible exception of the United States – which, as Evan Elkins shows, is shielded from the drama of geo-restriction due to its massive media complex – each country has its own set of policies and priorities around the geoblocking issue. In Australia and Canada, for example, a consumer rights discourse prevails, in which the main issue is the timely and affordable provision of digital content. The debate here is framed around windowing and discrepant pricing policies, leading to delays and price hikes for 'peripheral' English-language markets. This is what Tama Leaver calls 'the tyranny of digital distance', or the lag between first release in the center and availability at the edges.[11]

In Europe, the politics of geoblocking are quite different. With its dense patchwork of languages, borders and diasporas, Europe has long been a hotbed of unauthorised cross-border media consumption: people watch satellite TV signals meant for other nations, buy multiply-subtitled DVDs, and make shopping trips to neighbouring countries where prices are cheaper. This is an enduring feature of European consumption, one that has diminished little with the establishment of a single currency. While much policy attention is now directed at the creation of an EU Digital Single Market – in which all 28 EU member countries would share common pricing and availability for digital goods – intra-European variances in price and availability naturally persist.

11 Tama Leaver, 'Watching "Battlestar Galactica" in Australia and the Tyranny of Digital Distance', *Media International Australia* 126 (2008), pp. 145-154.

Within the European integration project, geoblocking is starting to be seen by as an anti-competitive – indeed, anti-European – technological restriction on free trade. Andrus Ansip, the former Estonian prime minister and current European Commission vice-president, has been leading the charge. Since 2014, 'tackling geoblocking' has been an official policy priority of the European Commission. Its Digital Single Market policy reads like a *Lifehacker* post: 'Geo-blocking leaves many Europeans unable to use the online services available in other EU countries, or redirects them to a local store with different prices… Such discrimination cannot exist in a single market.'[12] Here we see the 'merely cultural' issue of geoblocking framed quite seriously as a threat to continental capitalism and its cherished values of free trade, consumer rights, and smart regulation.

The politics of blockage and flow are different again in China, where a fast-growing domestic media sector – including a massive digital media production ecology – is overlaid with a carefully managed state system of site blocks, filtering and slow-downs, designed to temper demand for offshore services (especially Facebook and Google) and direct this inward to the local, regulated alternatives. For China the geoblocking issue is not so much the unavailability of content; when it comes to Chinese-language media and services, everything you would need is now inside the Great Firewall. Instead, it is about how and why certain user groups feel the need to climb this wall. As Jinying Li's chapter in this book evocatively describes, 'wall crossing' desire is widespread but unevenly distributed among the middle classes, and linked in complex ways to internal governance.

All this represents a new challenge for digital media theory, because it requires us to rethink some of the paradigms of control and censorship that we have inherited from earlier periods. Geoblocking, broadly defined, is a problem for many internet users in many countries, but to different extents, and for different reasons. It affects rich and poor alike, but can be circumvented easily for those with money or know-how. It interacts in complex ways with other kinds of internet phenomena, such as peer-to-peer piracy.

For example, we can see that the geoblocking issue has relatively little in common with the paradigm of the 'digital divide' that shaped discussion of the first decades of global internet use. Initially organised around a binary of use and non-use, with use concentrated in the developed world and non-use in the peripheries – and later developing into a more complex theory about the mutually reinforcing dynamics of class, infrastructure, education and state investment – the spatial imaginary of the digital divide has limited relevance to the problem of geoblocking. Nor is geoblocking a simplistic story of internet freedom versus internet censorship, that Western liberal vision of a free West against a censorious Rest. The new video geography does not cleanly follow any of these imaginaries.

As the case studies in the second section of this book show, the rise of circumvention practices around the world may instead be linked instead to the emergence of a transnational class who are using circumvention software for a mix of reasons – not just for "resistance",

12 European Commission, 'Better Online Access to Digital Services', http://ec.europa.eu/priorities/digital-single-market/access/index_en.html.

nor exclusively for consumption. This requires a variegated model of both access and politics. As Sean Cubitt argues, the question of access in internet culture needs to be understood through multiple registers simultaneously:

> The network society affords various kinds of access: to the rich consumer, video-on-demand (VOD), and to the genuinely wealthy subscription or sale models which avoid the dull necessity of paying attention to ads. For the Chinese masses, the protection of the Golden Shield; for the wealthy, Virtual Private Networks (VPNs) which fasttrack past the firewall like express check-in at the airport. For the ordinary punter, a data feed from Bloomberg; for the wealthy subscriber, real-time data on every stock for sale on every market.[13]

It may be that VPNs, proxies, and other geo-evasion technologies provide a set of popular technical competencies that are, taken together, laying the foundations for a global geo-circumvention system. This system connects politics with pleasure; connects censorship with consumption; embraces cutting-edge technologies while drawing on longer prehistories of cross-border arbitrage; and brings activists, file-sharers, hackers and mainstream users into unlikely and uncomfortable contact with each other. The politics of circumvention are anything but straightforward, as our authors illustrate. But in their complexity they provide the coordinates for a different map of cultural power, and a new way to think about the geopolitics of internet control.

References

Christophers, Brett. *Envisioning Media Power: On Capital and Geographies of Television*, Lanham: Lexington Books, 2009.

Cubitt, Sean. 'Telecommunication Networks: Economy, Ecology, Rule', *Theory, Culture and Society* 31 (2014): 185-199.

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

Deibert, Ronald et al. (eds). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*, Cambridge, MA; MIT Press, 2012.

Deibert, Ronald et al. (eds). *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge, MA: MIT Press, 2008.

European Commission, 'Better Online Access to Digital Services', n.d., http://ec.europa.eu/priorities/digital-single-market/access/index_en.htm.

Goldsmith, Jack and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*, Oxford: Oxford University Press, 2006.

Kompare, Derek. 'Adverstreaming: Hulu Plus', *Flow*, 24 Feb 2014, http://flowtv.org/2014/02/adverstreaming-hulu-plus/.

Leaver, Tama. 'Watching "Battlestar Galactica" in Australia and the Tyranny of Digital Distance', *Media International Australia*, 126 (2008): 145-154.

13 Sean Cubitt, 'Telecommunication Networks: Economy, Ecology, Rule', *Theory, Culture and Society* 31 (2014), p. 191.

O'Regan, Tom. 'From Piracy to Sovereignty: International VCR Trends', *Continuum: The Australian Journal of Media & Culture*, 4.2 (1991): 112-135.

Parks, Lisa and Nicole Starosielski. *Signal Traffic: Critical Studies of Media Infrastructures*, University of Illinois Press, 2015.

Paul, Ian. 'Ultra-popular Hola VPN Extension Sold Your Bandwidth for use in a Botnet Attack', *PC World*, 29 May 2015, http://www.pcworld.com/article/2928340/ultra-popular-hola-vpn-extension-sold-your-bandwidth-for-use-in-a-botnet-attack.html.

Roberts, Hal et al. *2010 Circumvention Tool Usage Report*, Cambridge, MA: Berkman Center for Internet and Society, 2010.

Roberts, Hal, Ethan Zuckerman, and John Palfrey, *2007 Circumvention Landscape Report: Methods, Uses, and Tools,* Cambridge, MA: The Berkman Center for Internet and Society, Harvard University, 2007.

Shadbolt, Peter. 'How Misbehaving at School Made One Man a Millionaire', *BBC News*, 18 May 2015, http://www.bbc.com/news/business-32702501.

Turner, Graeme and Jinna Tay. *Television Studies after TV: Understanding Television in the Post-Broadcast Era*, London: Routledge, 2009.

Wagman, Ira and Peter Urquhart. '"This content is not available in your region": Geoblocking culture in Canada', in Darren Wershle, Rosemary Coombe and Martin Zeilinger (eds), *Dynamic Fair Dealing: Creating Canadian Culture Online*, Toronto: University of Toronto Press, 2014, pp. 124-132.