6

The Proxy Wars

When considering how internet-distributed television has evolved globally, it is important to take into account the many informal user practices that have developed alongside, and in interaction with, the major platforms. Let me begin by offering a personal story that explains why this issue is significant for understanding Netflix. Like many TV fans in Australia—where Netflix was geoblocked until late 2015—I first experienced Netflix not as a local service but as a U.S.-based service that had to be accessed covertly by using a virtual private network (VPN). During these years of nonavailability between 2010 and 2015, several hundred thousand Australians covertly signed up for the U.S. Netflix service using a credit card, a fake U.S. residential address, and a VPN or other proxy service.[1] As long as our VPNs were active when we signed in, we could experience Netflix in the same way as Americans do. This workaround provided many happy hours of streaming until Netflix introduced an antiproxy policy in early 2016.

Australia was not an isolated case. In the early years of Netflix's internationalization, use of VPNs and proxy services was common in many countries—including Mexico, Canada, New Zealand, France, and Britain—where a local

Figure 6.1. Marketing for Getflix, one of the many DNS proxy and VPN services that facilitated unauthorized cross-border streaming (May 2016). Screenshot by Chris Baumann.

Netflix service was not available or where the local catalog was perceived as inferior to the U.S. version. Countless YouTube tutorials and websites offered step-by-step instructions on getting around geoblocking, making this a fairly mainstream practice. While all this was against Netflix's terms of service, the company did not seem to mind having the extra paying customers, and it all seemed like harmless fun.

My point here is that the history of Netflix as a global platform cannot be understood only as a tale of Silicon Valley innovation and international market entry. It is also, inevitably, a history of user experimentation, circumvention, and copyright infringement. These unauthorized practices are not just margin notes around the edges of the Netflix story; they are integral elements underlying the growth of Netflix as a global media service. Equally, the policies developed by Netflix to curtail this activity—the "proxy wars"—also form an important part of the wider institutional history of internet-distributed television.

User Practices and Platform Policies

In their influential work on Twitter, new media scholars Jean Burgess and Nancy Baym (2016) develop a "platform biography" approach to understand how platforms change over time. This involves attending not only to the features and design of a platform but also to how the platform is experienced, adapted, and transformed by its users. In the case of Twitter, it is well known that many popular user features—such as adding a hashtag to posts—were invented by users rather than platform designers. For Burgess and Baym, this raises the question of how everyday digital practices can "emerge . . . through user experimentation, as people seek to concretize the platform's emerging uses and norms, and in some cases to develop tools to enhance and better coordinate these conventions" (Burgess and Baym 2016, 10).

Extending this way of thinking to Netflix, we can start to appreciate the delicate back-and-forth between platform design and user activity that is a feature of most digital media. How have people variously used, adapted, and in some cases tricked the Netflix service? What tools and technologies have they employed to do this? Netflix is a relatively more closed platform than Twitter, but it is nonetheless amenable to a range of unofficial user practices. These run the gamut from innocuous platform hacks to more serious transgressions.

At the minor end of the spectrum, we find activities like *password sharing*, where users share their login credentials with friends, family, or strangers. This is a common practice: 40% of Netflix subscribers in the United States have reportedly let other people use their logins (Wallenstein 2013).[2] Other examples include uploading custom subtitles to Netflix or installing Chrome and Firefox browser extensions that add extra features to the Netflix website, such as IMDB (Internet Movie Database) ratings, random-play functions, microgenre browsing, or enhanced personalization. These user practices are uncontroversial and widely tolerated.

In contrast, geoblocking circumvention has proven to be a more troubling issue for Netflix and for entertainment industries generally. To understand why this is so, we need to know a little about the technology and business of geoblocking. This begins with the humble IP (internet protocol) address, the set of numbers assigned to a device that is used to send and receive data online. IP address "lookups" are a simple, cheap, and very widely used way to geolocate customers. Various free and proprietary databases have been developed for this purpose. Leading providers such as Akamai and Maxmind offer automated country-level and city-level geolocation databases, costing a fraction of a cent per query.[3]

From a commercial perspective, digital media platforms use IP geolocation because it offers a cheap and easy mechanism for market segmentation, personalization, and legal compliance (Svantesson 2004; Goldsmith and Wu 2006; Trimble 2012, 2016). Streaming services will typically check a user's IP address to confirm the user is in an authorized service zone. Outside this zone, the user will be confronted with an error message or an endlessly buffering screen.

IP geolocation is an imperfect system with many limitations, the most important being that geolocation can only tell you about the IP address of the device rather than the physical location of the person using it. Despite modest improvements over time, the system remains open to manipulation. As an Akamai representative has stated, IP geolocation "isn't meant [for] people are who trying to be evasive. . . . It's meant for the 99 percent of the general public who are just at home surfing" (Associated Press 2004).[4]

For the remaining 1%, various technical solutions exist to circumvent geoblocks and gain out-of-region access to online services (Lobato and Meese 2016). The most commonly used tools are VPNs, Smart DNS (domain name system) proxies, and free browser add-ons. VPNs, which can be used for privacy and business purposes as well as for circumvention, typically cost around US$5–$15 per month and provide an encrypted tunnel to a remote

TABLE 6.1. Popular DNS services used by Netflix's international subscribers, and their marketing slogans (circa 2015)

Service	Marketing Slogan
Unblock.US (DNS)	"Unblock Everything on Netflix, Spotify, Hulu and More"
uFlix (DNS)	"Expand your Netflix library!"
Proxy DNS	"Netflix, Sling, HBO, Hulu, and more . . . Outside USA."
Unotelly (DNS)	"Freedom. Security. Flexibility."
Blockless (DNS)	"Your Internet. Your Freedom."
MediaHint (DNS)	"Content Unblocked—Countries have borders. The Internet shouldn't."
Getflix (DNS)	"Unblock Netflix and Hulu Plus FREE with our 14 day trial"
Torguard DNS	"Unblock content anywhere"
TV Unblock	"American DNS codes"
Unlocator	"Watch Netflix anywhere"

server. There are hundreds of VPN suppliers in the marketplace, including well-known brands such as Private Internet Access, Hotspot Shield, and HideMyAss. Smart DNS proxies are cheaper than VPNs, costing a few dollars per month. They will effectively mask your IP address but do not encrypt your traffic. Finally, free browser add-ons such as Hola and MediaHint are easily installed and much simpler to use than VPNs or proxies. Users select from a list of countries, then choose an available video streaming service (e.g., selecting U.K. in Hola then allows the user to select BBC iPlayer).[5]

For simplicity, the rest of the chapter will use VPN as an umbrella term for these various circumvention tools, even though they are all technologically distinct. The next step in our analysis is to understand how Netflix responded to the rising popularity of these tools. We will then consider how the company's policies changed over time, and identify the strategies and values that motivated these changes.

Historicizing Netflix's Shifting Policies on Geoblocking

Netflix's internal policies on VPN use can be divided into roughly three periods. The first phase of internationalization, between 2010 and 2014, was characterized by a relatively permissive attitude. The second phase, between 2014 and 2016, witnessed growing external pressure to adopt a stricter policy. Finally, in 2016, Netflix introduced a new VPN-detection technology and recommitted to geoblocking as a principle.

During the first phase, Netflix was only available in the Americas and parts of Europe. Users outside these regions would see the message "Sorry, Netflix is not available in your country yet," and many used a VPN to get around this block. It is impossible to tell how many users accessed Netflix using VPNs at this time, but the practice was sufficiently well known for *Variety* to refer to Netflix's "black market diaspora" (Wallenstein 2014). The limited research literature also gives clues as to the cultural drivers of VPN use in various countries. Vanessa Mendes Moreira de Sa (2016) notes that tech-savvy Brazilian Netflix subscribers used VPNs to access the U.S. Netflix service because it offered English-language closed captions not available in Brazil (which was important for students). Studies by Leaver (2008), Beirne (2015), Stewart (2016), Shacklock (2016), and Lobato and Meese (2016) also show the prominence of geoblocking and circumvention in various other countries.

Netflix preferred not to comment publicly on VPN use at this time. The company was busy building a global brand with global market awareness. In fact, cultivating tech-savvy early adopters was part of its long-term strategy. Netflix enjoyed a reputation as a company that understood the internet and its users. It was reluctant to turn away paying customers, who helped to inflate the company's U.S. subscriber numbers and share price.

The second phase of Netflix's VPN policy was characterized by intense industry pressure. Rights-holders were starting to get anxious about what they saw as wholesale parallel importation or, worse, piracy. Tense conversations took place between Netflix, its suppliers, and its competitors. Concerns about VPN use were publicly aired in the trade papers and tech press, and were amplified by the publication of a number of reports (some rather speculative in nature) about the scale of the VPN "problem." One report by Global Web Index, "The Missing Billion," estimated that 28% of its global sample had used VPNs—amounting to "419 million people in GWI's 32 markets" (Global Web Index 2014, 9).

Armed with these statistics, many rights-holders pressured Netflix to take a tougher line on VPNs. "I know the discussions are being had . . . by the distributors in the United States with Netflix about Australians using VPNs to access content that they're not licensed to access in Australia," stated Simon Bush, CEO of the Australian Home Entertainment Distributors Association (Bush in Reilly 2014), "They're requesting for it to be blocked now, not just when it comes to Australia." By late 2014, all eyes looked to Netflix for a solution to the perceived VPN problem. The collateral damage from their laissez-faire approach was starting to mount as grumpy rights-holders continued to air their grievances.

The tension ratcheted up a notch in November 2014, when WikiLeaks released an archive of emails from Sony Pictures—including a leaked memo from Sony Pictures' chief digital strategy officer Mitch Singer, dating from December 2013—that revealed the depth of feeling within the studio about Netflix's lack of action on VPNs.[6] Noting that "this is a politically and emotionally charged issu[e] with Netflix," the Sony memo concludes that "Netflix can and should do a much better job geofiltering." Other leaked emails criticized Netflix's geolocation as "very leaky" and lamented its "reluctance to address this issue."[7]

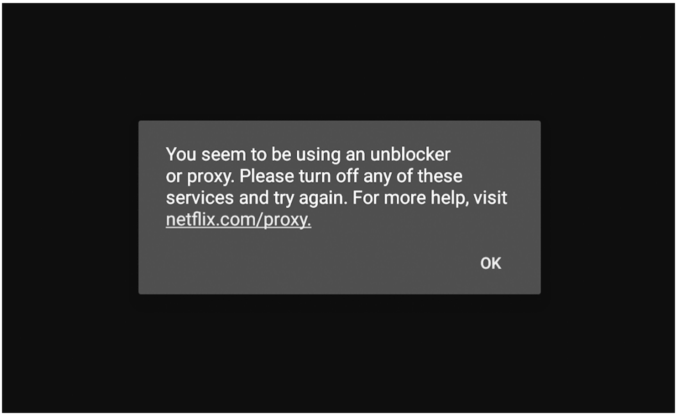
Rights-holders like Sony saw circumvention as a problem for at least two reasons. The idea of consumers wantonly "stealing" content from out-of-region services was naturally upsetting because it undermined the ideal of an orderly digital marketplace. VPN use seemed like an affront to the whole intellectual property system, and especially to the idea of territorial market segmentation—a foundational concept of copyright. Industry lobby groups began to speak of "VPN piracy," equating circumvention (which is actually more akin to parallel importation than piracy) with the specter of illegal downloading.

The second, more tangible concern was that VPN users were starting to dilute the value of content rights. If Canadian or British Netflix users could use VPNs to watch a particular program via the U.S. Netflix catalog rather than paying to watch it on a local Canadian or British pay-TV service, then major rights-holders (especially the Hollywood studios) would not be able to demand the same prices for their content that they were used to charging, because they could not guarantee territorial exclusivity. Whichever way you looked at it, rights-holders and distributors both had a lot at stake in territorial market segmentation. The geoblocking circumvention problem was showing just how crucial market segmentation was to digital media business models.

Asked about VPNs during a Netflix quarterly results call in April 2015, Ted Sarandos tried to play down the disquiet among suppliers. "Yes, [VPN use is] one of the many things that we have discussions with studios about on an ongoing basis, and we do continue to work with them, and work with the VPNs," Sarandos stated. "To be honest with you, it's kind of a whackamole to get ahead of the different usage of VPNs. It's become kind of a lifestyle thing for a very small segment of the population" (Sarandos in Netflix 2015a, 8). Rights-holders were not mollified by these remarks, and the pressure continued to build throughout 2015.

Finally, on January 14, 2016, Reed Hastings announced the global switch-on at CES in Las Vegas. Shortly afterward, Netflix issued a press release—"Evolving Proxy Detection as a Global Service"—announcing the introduction of an industry-standard geoblocking policy. Noting that Netflix's new status as a global service had removed the need for out-of-region access workarounds, the press release restated Netflix's commitment "to respect and enforce content licensing by geographic location," adding that "we look forward to offering all of our content everywhere"—a reference to the company's goal of achieving global licensing terms with its suppliers.

Shortly after the press release went out, internet forums lit up with commentary, criticism, and skepticism. Was Netflix serious about blocking VPNs? What technology would they use to do so? What would happen to the VPN industry, which thrived on consumer demand for cross-



You seem to be using an unblocker or proxy. Please turn off any of these services and try again. For more help, visit netflix.com/proxy.

Figure 6.2. Netflix error message for VPN users. Screenshot by the author.

border streaming? For the first few weeks, it appeared that nothing had changed. Most VPNs were still working as usual. On internet forums and social media, many gloated that Netflix's new VPN blocking system had failed. However, by the end of February 2016, most VPN users were seeing an unfamiliar and unwelcome message, shown in Figure 6.2.

Over the next few weeks, countless reports appeared on social media about VPN users being blocked from the U.S. catalog. Virtually all major VPNs seemed to be affected. Netflix's new proxy detection system was building up a dynamic database of IP addresses it determined were associated with VPNs and then blocking them all. Of course, there were still various ways to fool the system (VPN providers could actively change their IP address ranges, and tech-savvy users could set up a premium VPN subscription with an individually assigned IP address).

However, it was all starting to look too much like hard work to many users. Some decided it was not worth the hassle.

Meanwhile, VPN companies scrambled to come to terms with the new policy. Private Internet Access and Mullvad took the opportunity to distance themselves from circumvention, noting that they never endorsed such activity. Other VPN companies stuck to their guns. Torguard insisted it could still outsmart Netflix with its premium dedicated-IP service. The company's CEO stated that: "We greatly expanded our Dedicated VPN IP pool and now offer Dedicated IP options in over 55 countries worldwide. This has proven to work flawlessly for users who wish to bypass VPN blockades with geo-restricted streaming services" (Ernesto 2017a). Other providers quietly intimated that they would be able to work around Netflix's new policy. An Express VPN representative rather ambiguously stated "the first rule of Netflix is: do not talk about Netflix" (ibid.).

DNS proxy services were hit especially hard by Netflix's policy shift, because they relied heavily on the hardcore streamer user base. Several companies disappeared or morphed into VPN providers. Others experienced technical challenges. My colleague Chris Baumann and I tested a range of these DNS services in 2016 and discovered that, while the majority of them could still allow access to the U.S. Netflix catalog, they were not always reliable. Few services were consistently effective as circumvention tools, meaning that circumvention was now a fairly time-consuming activity that was likely to appeal only to the most committed users.

While certainly not bulletproof, Netflix's anti-VPN technology has been more or less effective in its stated aim. The blocking of VPNs changed the public perception of circumvention, making it appear difficult and bothersome instead of quick and easy. It also mollified the suppliers on whose content Netflix was absolutely reliant. In this way, Netflix was able to contain the perceived threat and redefine VPN use as a niche activity for hardcore geeks rather than mainstream internet users.

Making Sense of the Policy Shifts

Aside from the whack-a-mole games, what does the history of Netflix's VPN policy tell us about the relationship between user practices, technological restrictions, and company policies?

The digital media business is inherently leaky because it is built on the sale and leasing of access to infinitely reproducible goods, such as digital videos and ebooks. History tells us that what people do with these digital goods cannot easily be controlled, no matter how strong the digital rights management, so the imperative for forward-thinking media companies is not necessarily to stop all informal use of their property but rather to extract as much value as possible from a leaky market.

Netflix understood this well. Until 2016, its response to the VPN problem was not punitive. It was not about shutting down informal uses of its system. Rather, it was about extracting the maximum value from VPN users. This is why Netflix dragged its feet and carefully timed the introduction of its anti-VPN policy to align with the global switch-on—even though it had already known about the circumvention problem for years and rights-holder concerns had been growing for some time.

The trigger for the policy shift was economics rather than ideology. At a certain point, it made commercial sense for Netflix to stop thinking like a new-economy Silicon Valley company (committed to enhancing user experience through innovation) and to start thinking like an old-fashioned media company (by aggressively protecting its rights). The logic of the market dictated a cultural change in the company's values and self-identity. Netflix transformed from a "friend of the geeks" into an intellectual property defender because it made commercial sense to do so.

As further evidence of this shift, consider how Netflix's policies on illegal downloading have evolved in recent years. In public statements up until 2015, Reed Hastings took a moderate position on piracy, avoiding extreme antipiracy positions in favor of a pragmatic attitude that emphasized the importance of converting piracy into paid consumption. In 2013, Hastings stated:

> Certainly there's some torrenting that goes on, and that's true around the world, but some of that just creates the demand. Netflix is so much easier than torrenting. . . . We don't even think about trying to get rid of it. What we really think about is how to build an awesome service that people just want to use. (Hastings cited in Schellevis 2013)

Public statements like this—of which there are many on record by Hastings and other Netflix executives—suggest market realism rather than copyright puritanism. At this point in its history, Netflix wanted to present itself as a company that was reasonable, forward-thinking, and understanding of the internet and its users.

This relatively permissive attitude changed once Netflix became a major-league content producer. In recent years, Netflix has been aggressively enforcing its copyrights by

Reed Hastings on piracy and VPNs

April 2015: "The key thing about piracy is that some fraction of it is because [users] couldn't get the content. That part we can fix. Some part of piracy however is because they just don't want to pay. That's a harder part."

April 2015: "[VPN-enabled viewing is] certainly less bad than piracy. It's not something we encourage. It's actually very hard to detect, because VPN gets very good at covering their tracks for all the obvious reasons. And because we're focused on getting global very quickly, I think we'll see this issue disappear, and it will disappear because we'll be able to meet the demand directly in all the countries."

June 2015: "Well, you can call it a problem, but the truth is that [piracy] has also created a public that is now used to viewing content on the Internet. . . . We can think of this as the bottled water business. Tap water can be drunk and is free, but there is still a public that demands bottled water."

October 2016: "We've been very successful at finding technological ways of inhibiting the cross-border VPNs, which is roughly, like I'd mentioned, we didn't win the bidding for the Disney movies in the UK, so it's clearly not fair to allow our UK subscribers to watch the Disney movies from Canada or to the US. And so we found, with the help of the studios, some more technology that enforced their rights."

Sources: various press reports; Netflix quarterly earnings call transcripts 2015Q1 / 2016 Q3

sending out more than one million takedown notices to pirate websites (Google 2017). At the same time, it has expanded its legal team to include more copyright attorneys with antipiracy expertise. A March 2017 job advertisement for a Global Copyright Protection Counsel position at Netflix's Los Angeles office gives a sense of this work. In charge of "industry-wide anti-piracy strategic initiatives and tactical take down efforts with the goal of reducing online piracy to a socially unacceptable fringe activity," the counsel would be responsible for providing "detailed landscape and piracy trends analysis"; spotting "new trends and changes in the ecosystem"; lobbying; and providing "outreach" to pirate sites, sharing platforms, and social media services (Ernesto 2017b). In January 2018, Netflix and its partners in the Alliance for Creativity and Entertainment—including Amazon, HBO, BBC, and the Hollywood studios—also started filing lawsuits against suppliers of pirate streaming boxes (Ernesto 2018).

Antipiracy "education" was also part of the agenda. In 2017, Netflix also released a memorable antipiracy promo on YouTube, targeted at the French market. The subtitled video featured four *Narcos* cast members from the Cali Cartel, who threaten viewers with all manner of unpleasant deeds should they access *Narcos* illegally. "Hey you," intones Pêpê Rapazote, who plays the menacing character Chepe in the series, "Do you think we didn't see you Googling '*Narcos* season 3 download'?" Other cast members offer various warnings, such as, "If you want your entertainment, if you want your show, you gotta pay the Cali Cartel, *hijo de puta*," and "There is no please, no por favour, no *s'il vous plait*. . . . There's bullets for you, your family, and all the people you send to watch *Narcos* on those shitty websites full of pop-ups *sucios* [dirty]."

This was a new, humorous take on the old antipiracy advertising formula. While it stands in sharp contrast to Netflix's previous statements on piracy, this position makes sense when we consider what Netflix had at stake in its original content investment. By 2016, Netflix was spending billions of dollars on original content production each year. The company was now a major rightsholder, and it was starting to act like one—by introducing

Hollywood-style content protection and antipiracy policies. This investment in original content now colors every aspect of the company's strategy. Netflix wants to recoup this multibillion-dollar cost, enforce its rights, and minimize leakage in the system. Having orderly territorial markets and an effective antipiracy strategy is essential in this regard.

Cultural Consequences of the Proxy Wars

In this chapter, we have seen how Netflix progressively segmented its international markets into defined territories while users variously accepted, resisted, or circumvented this segmentation. A few years out from these events, and with the benefit of hindsight, we are in a position to answer some longer-range questions about these turbulent years: How did the "proxy wars" shape the evolution of television streaming as a global media practice? What did hundreds of thousands of internet users learn from the experience of using VPNs to access Netflix? Do these geoblocking battles have any wider relevance to internet culture?

It seems to me that one of the key legacies from these years has been an increased public awareness of the geography of digital markets. During the geoblocking and VPN debates, people started asking questions that showed some of the amusing inconsistencies of the copyright system. ("Why is this series available in Albania but not Alberta?" "Why can't I watch my favorite show online even when I'm happy to pay for it?") Many internet users experiencing geoblocking on a regular basis also came to form views on related issues like international price discrimination and windowing. In some countries, these concerns translated directly into government policy, as policymakers sought to constrain "unjustified geoblocking."[8]

Any user of a VPN or similar service during these years would have become familiar with marketing slogans promising "borderless TV" or the ability to "watch TV like a local." Meanwhile, Netflix catalog comparison sites such as AllFlix, FlixList, and Flixsearch encouraged users to consume media beyond their national borders. These websites were brazen about drawing attention to the disparities in the catalog system and promoting their own services as a workaround. A new popular discourse had emerged, characterized by a logic of cross-border comparison of digital media services and contempt for the principle of territoriality.

Catalog differences have eroded over time as more Netflix originals have been produced, but they remain significant in many users' minds. Unlike music streaming platforms, which enjoy global licensing terms, and social media sites, which are full of user-uploaded content that is not typically georestricted, Netflix was a global service with an obviously territorial catalog system. As such, it became a stalking horse for all the failings of territorial copyright generally, even though it arguably did more than most other companies to minimize them. In other words, Netflix came to stand in for a wider set of problems that were not of its making.

It is easy to dismiss all this controversy about VPNs and geoblocking as a first-world problem, and in some senses this is true: access to new-release movies and TV series is a privilege, not a human right. But to do so would also be to miss the subtle consequences of the events outlined in this chapter. The desire for a borderless Netflix inevitably helped to acquaint early adopters with digital rights and internet privacy discourses promoted by VPNs. It fostered a popular awareness of what are otherwise obscure technical matters. The common experience of geoblocking, leading to a desire for circumvention, operated like a "gateway drug" for a wider set of political issues.

The love affair with VPNs and cross-border streaming could be perceived as a degraded form of popular cosmopolitanism, in the sense that it involves a desire to cross borders and come into contact with media systems (or servers at least) in far-off lands. At the same time, this cosmopolitan impulse was also a symptom of cultural imperialism, because mostly what people were looking for when using VPNs to access Netflix was new-release American content. Regardless, it is safe to say that the rise of global Netflix helped foster in users a vernacular awareness of the geography of copyright and the contradictions of digital markets. The proxy wars may be over for now, but this genie cannot easily be put back in its bottle.