

Simon Lacey*

TRADE RULES AND THEIR LIMITS:

Internet Restrictions as Actionable Trade Barriers

Abstract

A number of legislative frameworks and policies exercise various constraints on access to the Internet for certain goods, services, and other content. Some of these are recognized by most, if not all, market participants as legitimate (data protection laws, measures to combat fraud, as well as the enforcement of intellectual property rights), whereas others are seen as merely disguised protectionism (onerous and/or opaque registration or licensing rules and the heavy-handed application of censorship policies to name just two).

This paper discusses the use that is increasingly being contemplated or made of trade rules, particularly WTO disciplines, to tackle those constraints that are viewed as either disguised protectionism or a breach of WTO commitments. It discusses the scope of these rules, the uses they have been put to in order to pry open services markets up to now, and the likely limits of their application.

It also looks at how those interests most concerned with exporting goods and services via the internet have recognized the limits posed by existing trade rules - at least implicitly - and how they are seeking to address these shortcomings by drafting new rules, either at the WTO or in *fora* such as bilateral and plurilateral trade agreements.

* IIEL Fellow at Georgetown University Law Center (lacey.simon@gmail.com | sl673@law.georgetown.edu)

Table of Contents

I.	INTRODUCTION - THE IMPORTANCE OF THE INTERNET IN GLOBAL COMMERCE	4
1.	From Cold War to E-Commerce	4
2.	Two Billion Customers	4
3.	The Global 500 and the Internet	6
4.	The Great Disruptor	6
II.	REGULATING THE INTERNET FOR BETTER OR WORSE	8
1.	The Instruments of Control - How Governments Regulate the Internet	8
2.	The Rationale behind Government Regulation of the Internet	9
3.	Good Internet Regulation and Bad	10
III.	RESTRICTIONS ON ELECTRONIC COMMERCE AND BARRIERS TO TRADE	12
1.	Some Definitional Issues	12
2.	The Google Manifesto on Free Flow of Information	13
3.	The European Union - United States Trade Principles for ICT Services	16
4.	The USTR National Trade Estimate Report on Foreign Trade Barriers	16
IV.	EXISTING TRADE RULES AND RESTRICTIONS OF INTERNET COMMERCE	18
1.	The Most Important WTO Rules for Challenging Internet Restrictions	18
2.	The Case being built by USTR against China	20
3.	The Importance of GATS Schedules and the Openness of Mode 1 Commitments	21
4.	The Narrowness with which GATS Exceptions are Interpreted	23
5.	<i>"China - Various Internet Restrictions"</i> - Strength of a Potential US Case	24
V.	THE NEXT GENERATION OF TRADE RULES ON INTERNET COMMERCE	25
1.	The WTO Work Program on Electronic Commerce	25
2.	The Trans Pacific Partnership	26
3.	The OECD Framework	28
4.	Possible Pushback from Some Developing Countries and Emerging Economies	28
VI.	FINDINGS AND CONCLUSIONS	30
	REFERENCES	31

Table of Abbreviations

AB	WTO Appellate Body
APEC	Asia Pacific Economic Cooperation
ARPA	Advanced Research Projects Agency
CERN	European Organization for Nuclear Research
DSU	WTO Dispute Settlement Understanding
FCC	United States Federal Communications Commission
GATT	General Agreement on Tariffs and Trade
GATS	General Agreement on Trade in Services (of the WTO)
ISP	Internet service provider
NBP	National Broadband Plan
NCSA	National Center for Supercomputing Applications
NSF	National Science Foundation
OECD	Organization for Economic Cooperation and Development
P4	Trans-Pacific Strategic Economic Partnership Agreement
RMB	Renminbi (currency of the People's Republic of China)
TPP	Trans-Pacific Partnership
USTR	United States Trade Representative
VoIP	Voice over Internet Protocol
WTO	World Trade Organization

I. INTRODUCTION - THE IMPORTANCE OF THE INTERNET IN GLOBAL COMMERCE

1. From Cold War to E-Commerce

What started as an experimental research network created by a US Defense Department research agency gradually evolved into a platform for information exchange within America's academic and research communities. Like the social networking site *Facebook* would do some ten years later, the Internet then moved from being a platform used solely by those in academic circles to the mainstream of the world's businesses and households, to become what it is today, namely an invaluable tool for any action or process that involves information and/or communication and that many of us take for granted, but simply could no longer imagine living without.

The Internet today has evolved considerably from its early beginnings (in 1969) as an effort to share scarce computer resources among researchers working in institutions across the United States for the Advanced Research Projects Agency (ARPA). In 1990, researchers working at the European Organization for Nuclear Research (CERN) invented the World Wide Web. This innovation transformed the Internet from a medium of purely text-based exchange to one in which information could be organized and presented in various formats (including multi-media). It also made the resources of computers linked to the Internet all over the world accessible through a single, simple interface. The work done in this context at CERN also resulted in the development of the first basic Web browsers, the underlying software for which CERN released into the public domain in 1993. It didn't take long (1992) until Web servers were set up at other centers around the world engaged in physics research, including the US-based National Center for Supercomputing Applications (NCSA) at the University of Illinois, which was funded by the National Science Foundation (NSF). It was researchers at the NCSA who developed Mosaic, the first widely used graphical Web browser, several of whose developers went on in 1994 to found Netscape. The NSF for its part, had also established (in the mid-1980s) and was operating its own high-speed network in order to link up its supercomputer centers, in addition to a number of national laboratories. This network was known as the NSFNET.

The final piece of the puzzle, i.e. the transition from a global network of computers principally serving researchers to a commercially exploitable platform was the emergence, over time (throughout the 1980s and early 1990s) of private sector involvement, first through the organizations that built and operated the NSFNET backbone (IBM, MCI and Merit) and then through an early generation of commercial Internet service providers (ISPs), and by the NSF's plan, published in 1991, to have the Internet infrastructure taken over by several competing commercial operators. Today, the backbone infrastructure that comprises the Internet is spread through almost all the nations of the world and the Internet has transformed the lives of billions of the planet's citizens by making information and communications infinitely faster, easier and cheaper for anyone who can obtain access to it.

2. Two Billion Customers

A 2011 study by the McKinsey Global Institute¹ provides some impressive numbers as evidence of the importance of the Internet today. For example, it estimates that there are currently 2 billion people regularly using the Internet, and that close to \$8 trillion changes hands each year through e-

¹ McKinsey Global Institute (2011).

commerce.² It also notes that in some developed country markets, approximately two-thirds of all businesses have some kind of web presence, and that more than 75 percent of the value added created by the Internet is in what it refers to as "traditional industries". Even behind the numbers there are other, less easily quantifiable but equally perceivable effects that the Internet has had on the lives of many who live in those countries where its spread has been the most pervasive. As McKinsey notes, "the Internet has made the world flatter by allowing instant access to an almost endless stream of information that can be immediately brought into play".³ Perhaps the most astounding statistic, is that the Internet has generated as much economic growth in the last 15 years as was generated by the Industrial Revolution in 50 years.⁴

Google (2010) also notes the empowering effect the Internet has had, allowing businesses even in more traditional sectors to change many facets of their organization and operations and reach international markets in a way that was much costlier and generally more burdensome only two decades ago.⁵ Google describes the Internet as a "general purpose technology enabler - a once-in-a-generation technological development that fundamentally changes how economic activity is organized and enables a productivity leap".⁶ More importantly, the Internet economy is a significant contributor to US GDP, a dynamic driver of economic growth for the US economy, and the source of millions of jobs. An obvious conclusion underlying the importance of the Internet to the US economy is also the relative strength of US companies in the Internet economy and in the online ecosystem. The digital economy is one where the US has a solid comparative advantage, and where many US firms are competing on both domestic and foreign markets from a position of relative strength.⁷ Any attempt to disrupt the functioning of the Internet can thus also be perceived as an encroachment on US comparative advantage. This is really the not too subtle theme underpinning Google's 2010 manifesto for a world free of overly restrictive and opaque Internet restrictions.

But the US is not the only country with a strong online sector. Other developed countries, predominantly in Europe and Asia have largely followed the US down the road of adopting the Internet as a transformational platform for governments, businesses and consumers. Thus the United Kingdom and Sweden are perceived as being the most advanced countries in terms of the online ecosystem in Europe, whereas in Asia, South Korea (a world leader in broadband penetration rates) is ahead of Japan in becoming a major force in the global Internet economy. Both India and China are quickly increasing their share of the global Internet economy, and firms in these countries are achieving similar successes to their counterparts in more developed and mature Internet economies in exploiting the opportunities this technology provides, both in their home markets and abroad.

² McKinsey Global Institute (2011), p. 9

³ McKinsey Global Institute (2011), Executive Summary at p. 1.

⁴ Ibid, Executive Summary at p. 3.

⁵ Google (2010), p. 2.

⁶ Ibid, p. 3

⁷ This is also a point the McKinsey report makes in no uncertain terms: see McKinsey Global Institute (2011), Executive Summary at p. 4.

3. The Global 500 and the Internet

If one takes the time to look up which companies today are in the Global 500⁸, it quickly becomes obvious that many of them are either technology companies whose products form the building blocks of the Internet (Hewlett-Packard, Apple, Cisco), communications companies whose business models have been transformed by the Internet and whose services include providing consumers and businesses access to the Internet (AT&T, NTT, Verizon Communications), or financial institutions who rely on the Internet for large chunks of their business processes and client interaction (Bank of America, Allianz, BNP Paribas). In addition to these, some of the most ubiquitous global brands and oft-used products and services are provided by companies who are first and foremost Internet companies and who only emerged because they were successful in harnessing the power of the Internet as a platform to promote themselves and what they were offering (Google and Amazon, both already in the Global 500, as well as fast-growing firms such as Facebook and Expedia).

4. The Great Disruptor

The Internet, despite being a boon for many economic sectors, for productivity and for economic growth in general, has nevertheless been a highly disruptive technological innovation and the costs/benefits of the changes wrought by it have been unevenly distributed. Nobody working at Borders in the 1990s would ever have imagined that within less than 20 years the prime retail locations they occupied in cities across the country and indeed across the world would be abandoned almost overnight because of the company's inability to adapt to both (1) the possibility provided by the Internet to browse, sample and purchase books online and have them delivered overnight to a customer's home as well as (2) the even greater innovations of digitalizing print media and inventing electronic book readers like Amazon's Kindle.

The industries or sectors where the Internet's impact has arguably been the greatest (or most disruptive) would have to include:

1. **Selling and distribution of goods** directly to customers, where the online retail industry has become so large that online services like Amazon have put their brick-and-mortar competitors like Borders, out of business;
2. **Selling and distribution of music and films**, where digitalization of these media have transformed distribution networks, first through unauthorized file-sharing services and protocols like Napster and BitTorrent, but now also through legal means. The losers here have been record labels and film studios (both industries were slow to adapt) but the winners include companies like Apple's iTunes and Netflix;
3. **Print media and newspaper publishing**, where the online editions of most newspapers attract a far larger viewership than do the print editions, and where digitization has also transformed distribution of books, so that Amazon's Kindle and Apple's iBookstore have come to establish themselves as the dominant players in this new medium (two services that didn't even exist twenty years ago);
4. **Retail banking and payments** with most customers performing the lion's share of their day-to-day banking transactions through their bank's online portal and with online payment

⁸ http://money.cnn.com/magazines/fortune/global500/2011/full_list/ (April 26, 2012).

services such as PayPal also coming to assume an important place in the e-commerce ecosystem;

5. **Telephony, with Voice over Internet Protocol (VoIP) services rapidly displacing conventional long-distance fixed line communications and already carrying a substantial and growing share of international voice traffic.**

In short, there is hardly an area of activity in modern day life involving either information or communication that isn't done primarily via the powerful and omnipresent platform that the Internet has quickly become. Because of its all-pervasiveness, it only seems natural that the Internet should be regulated in one form or another. In the next chapter, I explore some of the regulations to which the Internet is already subject and some of the ways these regulations also constitute restrictions on commercial activities undertaken via or with the help of the Internet.

II. REGULATING THE INTERNET FOR BETTER OR WORSE

1. The Instruments of Control - How Governments Regulate the Internet

Governments regulate electronic commerce and the internet in various ways and for various purposes. Regulation may also be directed at different aspects of the Internet, from access to the Internet, functionality of the Internet and online activity.⁹ Regulating access to the Internet is as much about controlling the conditions subject to which ISPs can operate (and thus users can avail themselves of these services), as it is about intervening further upstream by controlling access to and use of the physical backbone infrastructure without which there would be no Internet. Regulating functionality is about intervening to control the technical quality of Internet connectivity either by exercising influence over such factors as bandwidth and speed, communications software, and technical protocols.¹⁰ Finally, governments intervene to regulate online activity, either by enacting laws to make certain activities or content illegal, by filtering, surveillance and more subtle forms of control, like trying to influence and manipulate the dialectic space in which ideas, perceptions and the like are exchanged via various online platforms.

Whereas it may be true that no entity, public or private, has complete control over all aspects of the Internet¹¹, it is equally true that the monopoly on the legal use of force and coercion that governments enjoy within their own sovereign territories also affords them an enormous range of policy instruments to exercise control over the whole ambit of actors in the online ecosystem, from those who build and operate the physical infrastructure, to those that provide downstream internet access services, to those that use those services to offer for sale other services, and finally to those who consume these services, the end-users or consumers. Because governments enjoy jurisdiction over all those who live, work and/or do business within their respective territories, governments can and do have the power to regulate. They enact laws banning certain online content and activities and have the physical and institutional capabilities to enforce those laws against those who break them. Governments have the power to grant licenses to those who wish to provide online services, and what governments grant, they can also take away. Thus governments can coerce ISPs or other commercial entities that store, organize and retrieve information at the request of users (say Internet search engines) to refrain from allowing users to access content on certain sensitive subjects, and governments can penalize these commercial entities by revoking their operating licenses when they fail to comply.

In short, just like there are countless ways for a government to tax its citizens, the ways for a government to regulate the Internet within, and in some cases beyond its borders are just as innumerable. Many of these ways represent perfectly legitimate policy objectives and are largely harmless. In fact, in many ways, government regulation of the Internet is a perfectly desirable and necessary tool of executive authority. Without it, we would all undoubtedly be much worse off. However, like any area of regulation, governments can sometimes regulate beyond what is strictly necessary or useful, and governments can also intervene for policy objectives that are less than legitimate. Finally, like any area of regulation, regulating the Internet is also prone to capture by

⁹ See Eriksson and Giacomello (2009), p. 206.

¹⁰ Ibid.

¹¹ Wu and Goldsmith (2006), p. 21

well-organized and narrowly focused economic interests seeking to maximize their own welfare at the cost of that of the public more generally. Several of these instances of over or improper regulation are discussed in more detail below.

2. The Rationale behind Government Regulation of the Internet

Governments in many countries intervene by regulating the Internet for a whole range of public policy objectives. One such objective is to uphold property rights, namely intellectual property rights. One (arguably unintended) consequence of the ease with which the Internet makes information accessible is the corresponding scale of copyright piracy that is perpetrated over the Internet. An example of the enforcement of copyright against Internet piracy was the recent taking down of the online virtual library "library.nu", following court injunctions obtained by a coalition of publishers.¹² Protection of private citizens' intellectual property rights was also the driving policy objective behind recent efforts in the US Federal legislature to enact the Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA), which ultimately failed in the face of massive public uproar and controversy over what many feared was a case of regulatory over-reach.¹³

Another reason why governments intervene and regulate the Internet is to uphold and enforce laws intended to protect certain vulnerable elements of the population. This would include children, and the very strict laws against child pornography on the Internet are both intended to enforce the child pornography laws (themselves intended to protect children from this form of abuse) as well as to protect public morality (since the sexual abuse of minors is universally condemned as morally repugnant). Government efforts against those who use the Internet to distribute and view child pornography have resulted in some very high profile criminal convictions, such as that of the English Glam Rock celebrity Gary Glitter in 1999.¹⁴ Government efforts to uphold public morality are in fact, the stated public policy objective behind most censorship legislation, and the Internet is a platform over which governments have tried to enforce censorship laws in various ways, and in many countries.¹⁵

Protection of privacy is another public policy rationale often found at the heart of governments' efforts to regulate the Internet, and these efforts are usually directed at policing the kind and amount of information companies can collect and share regarding the personal identities and online habits of private citizens. In this context, one recalls the furor Google caused when it was found to be collecting and storing data from unencrypted home wireless networks while collecting photos of neighborhoods and localities for its Street View service, an incident which led to criminal investigations in a number of countries.¹⁶ Part of the concerns motivating these government regulatory efforts are the individual human rights of citizens (privacy is after all a right, even in the age of Facebook) while another element of these efforts is combating such negative phenomena as identity theft and fraud. Thus these efforts are in part also motivated by government efforts to either protect the rights and property of its citizens and/or enforce laws against criminal conduct.

¹² Kelty (2012).

¹³ See for example BBC (2012) for what can probably be considered a more "balanced" portrayal of the different issues and stakeholder interests involved.

¹⁴ See Bennetto and Judd (1999).

¹⁵ See Palfrey (2010).

¹⁶ Hansen (2010).

The Internet also sees intervention in the form of government regulation in order to stop or hinder incidents of computer hacking (which can result in the theft of valuable information or business secrets that are otherwise protected by the law) or the spreading of malicious software, which is capable of wreaking untold damage to computer networks and thus public and private infrastructure. Here the public policy goals pursued include maintaining the integrity of vital infrastructure (thus involving national security concerns) but also aim to mitigate the high cost to the economy as a whole that such hacking or malicious software can cause. The recent efforts to shut down WikiLeaks and cut off its funding, carried out by private domain name, hosting and payment service providers under considerable pressure from US officials, were motivated primarily by national security concerns,¹⁷ but prosecuting hackers who release computer viruses that quickly spread all over the world is usually done as part of general law enforcement.

Yet another sub-set of public policy concerns that see the government actively intervening to regulate the online ecosystem is to promote competition and to ensure that no single, or a small group of economic operators are in a position to exercise market power in a way that would undermine the Internet's effectiveness as a platform to exchange goods, services and ideas. This was in evidence recently when the Department of Justice filed an antitrust suit against Apple and five major publishers, alleging a conspiracy to fix the prices of electronic books.¹⁸ The concerns underlying the US governments' policy objectives in this context seem to stem from an accepted position that competition on markets is generally a positive phenomenon and that the Internet is no different. This was certainly on display in 2010 as the Federal Communications Commission (FCC) sought to fulfill a mandate entrusted to it the previous year by Congress and formulate a National Broadband Plan (NBP).¹⁹ The FCC's position when conceptualizing the NBP also seems predicated on the realization (discussed above) that the Internet is a very important engine of the economy and thus both a driver of economic growth as well as a source of US economic competitiveness. Maintaining these are clearly a public policy objective as was very much in evidence under Congress's original mandate to the FCC to design the plan as part of the American Recovery and Reinvestment Act of 2009.²⁰

3. Good Internet Regulation and Bad

A detailed theoretical framework exists on what should be the principles guiding and constraining regulatory interventions, and it is not the purpose of this paper to delve into this framework here. Suffice to say that it is generally recognized that governments should choose the correct regulatory instrument to meet the policy objective being sought and the benefits of a given regulatory approach should be weighed against the costs such an approach would likely impose (in terms of administration and compliance). Other watchwords are frequently heard in the context of

¹⁷ See Halliday and Arthur (2010).

¹⁸ Chang and Puzanghera (2012),

¹⁹ Federal Communications Commission (2010).

²⁰ Congress's mandate to the FCC was to develop a NBP that would allow Americans to maximize use of broadband in advancing "consumer welfare, civic participation, public safety and homeland security, community development, health care delivery, energy independence and efficiency, education, worker training, private sector investment, entrepreneurial activity, job creation and economic growth, and other national purposes", thus a very long list of public policy objectives contingent on faster access to the Internet. See FCC (2010), Executive Summary, p. XI.

internationally recognized best practices for regulatory policy, such as: consultation (of all those who may be impacted by a regulation); equality of opportunities to participate in the consultation process; transparency of the regulatory process; easy access to regulation and regulation formulated in terms that are easily understandable to everyone; simplicity, clarity, and predictability of regulation.²¹

In some ways, whether or not the specific manner in which the Internet is regulated is good or bad is simply a matter of perspective. Regulations which restrict a person's right to use the Internet to engage in, distribute, or access hate speech directed at a certain minority are almost certainly viewed as "good" by the minority towards whom such speech is directed, but will simultaneously be viewed as "bad" by those doing the hating.²² In the same way, regulation that restricts foreign service providers' freedom to operate commercially using the Internet will be viewed as "bad" by the foreign service providers in question (and perhaps even their customers) but will probably be viewed as "good" by their domestic competitors who are firstly not negatively impacted by the regulation and, secondly will be relieved that they have less (or no) foreign competition to contend with.²³ Even the most benign and general welfare enhancing regulation might be viewed as undesirable by those who must bear the costs of complying with it, particularly if they feel these costs are disproportionate to the regulatory objective being pursued, or are disproportionately borne by them compared to other stakeholders.

This paper is predominantly concerned with Internet regulation that manifests itself in the form of restrictions constituting barriers to trade. These restrictions are trade barriers in that they either hinder market access for foreign service providers or tilt the market or regulatory playing field against foreign service providers in a way that negatively distorts the competitive environment they must operate in. Either way, the Internet restrictions discussed in this paper are discriminatory and they impair effective competition. They are also arguably in breach of international trade rules, i.e. binding treaty commitments that members of the World Trade Organization have entered into. For these reasons, they can probably be considered "bad" within the meaning discussed here, although again this is a matter of perspective. They are predominantly bad for the commercial entities they negatively impact, but they might also be bad for customers and bad for the economy of the countries imposing them. They are "good" for the narrow set of well-organized domestic political economy interests that have in many cases conspired and lobbied to have them put in place, or to at least have them implemented in the specific manner in which they impact the economic sectors they regulate. I take up this topic in more detail in the next chapter.

²¹ These from OECD (2010), pp. 6-8.

²² See Meller (2001).

²³ See George-Cosh (2011) for a discussion of the UAE government's steps to lift the longtime ban on Skype.

III. RESTRICTIONS ON ELECTRONIC COMMERCE AND BARRIERS TO TRADE

1. Some Definitional Issues

The term Internet commerce here is understood in a broader sense than just electronic commerce, which focuses on transactional exchanges done by electronic means, between two parties that are in geographically different locations. Internet commerce for the purposes of this paper means any commercially relevant activity or activity engaged in for commercial purposes over the Internet, regardless of whether or not they are specifically directed at culminating in a given transaction.²⁴ Internet commerce is a broad and overarching term that encompasses electronic commerce but also much more. Thus Amazon's online retail service, which started off selling books but which now sells almost anything, is an example of an e-commerce business and thus also a part of Internet commerce. Twitter on the other hand, is certainly an important stakeholder and player in Internet commerce, but probably does not consider itself as being an electronic commerce business, because it doesn't sell anything to its users. The distinction is not extremely relevant for the purposes of this paper (although many policy initiatives at the international level focus solely on electronic commerce), but it is arguably worth getting definitions straight.

Some restrictions that may appear to be Internet restrictions are really just restrictions that affect any transaction involving a given product or product type. Thus an individual who is blocked from selling nuclear centrifuges on, say, eBay, is not the victim of an Internet restriction *per se*, but rather a general ban on selling devices and materials that can be used to build a nuclear bomb. Thus anyone trying to sell a nuclear centrifuge on eBay will not have to wait very long before a law enforcement agent comes knocking, and eBay will have to remove the offending offer.²⁵ A similar situation exists, say, where a government has a policy of not allowing a certain religious movement to be practiced within its territory, as is the case in China with Falun Gong. The fact that Falun Gong cannot use the Internet in China to promote its beliefs, try and obtain new converts, raise funds, or engage in any other activity, is not so much an Internet restriction *per se*, but rather the logical extension of a policy that is implemented across all public media (newspapers, television and radio advertising etc.). A milder variant of the same phenomenon can be found in liberal democracies: Germany, for example, does not ban the Church of Scientology, but keeps it under observation by its domestic intelligence service, and that scrutiny extends to the Church's online activities.²⁶ Equally, the fact that Google China was required to self-censor references to Falun Gong in its search results was not so much an Internet restriction *per se*, but just the logical extension of the Chinese Communist Party's unrelenting campaign against what it considers to be a dangerous religious sect.²⁷

²⁴ Note that the Work Program on Electronic Commerce within the WTO has come up with a definition of electronic commerce as "the production, distribution, marketing, sale or delivery of goods and services by electronic means" although it notes that this definition is "exclusively for the purposes of the work programme, and without prejudice to its outcome"; see http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm (April 26, 2012).

²⁵ This has happened several times in the past in the context of people trying to sell Nazi paraphernalia on eBay; see Virzi (2001).

²⁶ See "Germany Will Continue to Watch Scientologists" in Spiegel Online International Edition <http://www.spiegel.de/international/germany/0,1518,535049,00.html> (April 26, 2012).

²⁷ McGregor (2010), p. 82.

2. The Google Manifesto on Free Flow of Information

The Internet restrictions that have emerged as the most consistently recurring and commercially damaging tend to fall into a narrow range of measures of either a technical or legal nature and are directed almost exclusively at the Internet presence or activities of the economic operators they are seeking to affect. Google (2010) categorizes and lists the "four basic strategies" that governments have tended to rely on in order to restrict the flow of information on the Internet.²⁸ The first of these involves rendering a given Internet service totally inaccessible (something that Google refers to as "technical blocking"²⁹ but which is something also referred to as "filtering") or disrupting access to certain key terms, web pages or entire Internet domains. This is the case with Facebook in China and many other countries, and was also the case in Turkey, which for a period spanning more than two years pursued an aggressive campaign to block access to YouTube for Turkish users due to a number of videos posted on the site which the Turkish Government perceived as violating domestic laws intended to posthumously protect the reputation of the founder of modern Turkey, Mustafa Kemal Atatürk.³⁰ In the same manner, a recently introduced policy in Indonesia entitled "Internet sehat" or "healthy Internet" attempts to block all users within Indonesia from accessing any websites containing pornographic materials (a government policy that is quite common throughout the Islamic world, although mandatory filtering of this kind remains highly controversial in most liberal democracies because of laws guaranteeing freedom of expression, as the debate over the Australian government's proposed mandatory Internet filter has shown).³¹

The second of the four basic strategies referred to by Google (2010) involves licensing laws and requirements which governments use in order to exert influence over the Internet and restrict the ability of commercial operators to use the Internet for their particular commercially related purposes. The problems which regularly surface in this context do not relate to the licensing requirement *per se* (although in most liberal democracies a license is certainly not usually required to operate a website unless this is done for the purpose of selling services that fall under a regulated sector, like medical services, or financial services), but rather the arbitrary and opaque manner subject to which the licensing regime in question is administered. This is more of a rule of law or due process issue, and these regimes can be found wanting in many countries as much due to the dubious policies of governments as to the lack of developed administrative or institutional capacity. The best known example of this involved Google, whose license to operate a Chinese service within China came under threat once the company decided (in 2010), to stop censoring search results and instead to redirect users of its search engine to Google Hong Kong.³²

The third strategy cited by Google in its 2010 manifesto is the practice of governments to issue take-down orders, forcing entire domains to be taken down. The problems associated with this form of Internet restriction are essentially two-fold. First the practice itself is a very heavy-handed form of censorship. Second the legal regime under which and the way such orders are issued and enforced

²⁸ Google (2010), p. 5.

²⁹ Ibid.

³⁰ Ibid, p. 6.

³¹ See "Blackberry maker says will filter porn to meet Indonesia rules" at <http://uk.reuters.com/article/2011/01/10/us-indonesia-internet-idUKTRE7092DK20110110> (April 26, 2012),

³² See "Google quits redirecting China Web traffic to Hong Kong" in *USA Today* online edition at http://www.usatoday.com/tech/news/2010-06-29-google-china_N.htm (April 27, 2012).

may leave a lot to be desired. The first of these problems relates to the principle of proportionality in administrative action. Ordering the take down of an entire website will in many cases go well beyond what is required to achieve the desired policy objective, unless the website's only purpose is to engage in illegal activity - similar to the case alluded to above where the "library.nu" virtual online library was taken down, because its sole purpose was the dissemination, in digital form, of pirated works. Still, even in the case of "library.nu", a less severe measure might have been imposed than simply taking down the website, such as forcing users of the site to pay the royalties owed to the authors or right holders of the copyrighted works. The second issue that arises in this context is similar to that discussed immediately above, namely shortcomings in the legal system that issues the order, and which may fail to afford affected parties sufficient opportunity to defend themselves, or to seek legal redress against such an order once issued.

The fourth strategy cited by Google is where governments attempt to induce companies to practice self-censorship through various methods which can include "surveillance and monitoring, threats of legal action and informal methods of intimidation". Here again, Google seems to itself be the main victim of this category of restrictions, and its experience in China will have colored its views on this issue. The legal action it refers to would surely include revocation of its business license but might also include more serious charges being brought if some of the content it disclosed in violation of self censorship requirements was deemed to fall under national secrecy³³ or other criminal law legislative frameworks, such as Thailand's notorious lèse-majesté laws. Another problem of this sort of strategy is that it increases the uncertainty of the regulatory environment companies operate in, so that Internet restrictions of this kind represent a source of regulatory risk that is often hard to reasonably assess, predict or develop mitigation strategies for in countries without a properly functioning and independent judiciary.³⁴

The 2010 Google manifesto goes into some detail on the commercial and economic damage that such Internet restrictions can inflict, including undermining the integrity of what has become a key "trading route" of the global economy in the 21st century.³⁵ It also mentions the fact that these restrictions can do damage to companies seeking to enter new markets,³⁶ unfairly advantage local companies allowing them to gain and maintain market share that they might otherwise not enjoy, impeding the effectiveness of business operations of companies by creating an additional source of uncertainty and unpredictability, undermining companies that use the Internet as their main platform to advertise and distribute their goods and services, as well as damaging downstream operators that rely on the Internet in order to be able access mission critical services and other inputs they require in order to operate. Finally, Google mentions the broader damaging systemic effect that pervasive Internet restrictions can have on the architecture and functioning of the Internet as a whole and thus its ability to be a platform and engine of innovation and growth.

Google (2010) also goes on to elaborate on a number of other grievances that it alleges are perpetrated by many governments around the world and which tend to make commercial

³³ Barboza (2009).

³⁴ This is almost certainly the case in China, where the judiciary is deemed by many observers to be little more than an extension of the Communist Party's control over all aspects of the country's governance; see e.g. McGregor (2010) p. 15.

³⁵ Google (2010), p. 8.

³⁶ Ibid.

operations very difficult for economic operators who rely on the Internet across various parts of the value chain (whether it is advertising/marketing, sales/distribution, or even supply chain management). These include an opaque and constantly changing regulatory environment, which makes compliance both difficult and expensive and also increases uncertainty for economic operators, particularly foreign based or foreign owned ones. Another grievance Google notes is the "wholesale blocking of services", and lists among the victims here video upload/download sites, social networks and platforms for online blogging. Facebook and Twitter are perhaps the best-known examples of this, and have usually faced wholesale blocking in countries run by more autocratic regimes, generally for (the not wholly unjustified) fear that they would be used by political opposition groups to mobilize and organize support against the regime. The 2008 US presidential election was perhaps the first where, given the importance of the so-called "youth vote", social media was a major part of at least one candidate's campaign, with some very high-profile individuals from the social media industry being recruited to join and lead this aspect of then Candidate Obama's campaign. Putting politics aside, at the time of writing, Facebook is preparing to go public in a much anticipated initial public offering that will undoubtedly raise several billion dollars for the online social network company. Using wholesale blocking to keep Facebook out of China, while allowing a home-grown alternative to thrive in the form of RenRen, is more than just an issue of resisting what some Chinese leaders might see as US cultural imperialism or assuming and maintaining control of the online dialectic space, it is also very much a dollars and cents issue, one involving real money and one that undercuts US comparative advantage in an economic sector that it currently clearly dominates and is likely to keep dominating for some time.

Yet another complaint that Google voices, and this is really at the heart of any trade dispute (and thus the present analysis), is what it terms "bias against foreign competitors" but what in trade law parlance is referred to as a violation of the national treatment principle. There are many examples of this, and again, they seem to focus predominantly on China. Facebook has already been discussed above, but other examples include the various efforts by Chinese authorities to steer Chinese Internet users away from the search engine websites of US owned companies like Google, Microsoft and Yahoo, to the Chinese-owned search engine Baidu. A more subtle example of this would arguably be the huge defeat suffered by eBay on the Chinese market at the hands of Chinese Alibaba (Taobao). Several commentators have noted that eBay's rout on the Chinese market was caused by several factors, not least of which was the company's inability to better tailor its service to local markets. eBay suffered a similar fate in Japan and India, but not Korea.³⁷ But other commentators have listed the complexity of the regulatory regime governing the Internet as well as the hard time foreign commercial operators generally suffer at the hands of Chinese regulators. As one expert on China noted following a struggle with his own regulator "... with one part or another of the Chinese government having its fingers in every aspect of business in China, if your regulator is not your competitor, it is likely that your regulator is dedicated to helping your Chinese competitors."³⁸

³⁷ See Purkayastha and Faheem (2008).

³⁸ This quote from James McGregor, who as the Beijing Bureau Chief of Dow Jones, had to fend off an attempt, in 1996, by Xinhua to take over the business of all foreign financial news providers in China. After being beaten back in its first attempt to do this, the Chinese regulator made another play at the same market almost exactly ten years later before again being beaten back. The quote is from McGregor (2005), at p. 142.

3. The European Union - United States Trade Principles for ICT Services

A joint declaration issued by the EU and the US on "Trade Principles for Information and Communication Technology Services"³⁹ (discussed in more detail below in the context of the WTO Work Program on Electronic Commerce) also provides some insights into the kind of regulatory restrictions that threaten to impede international trade and which have been put onto the respective trade policy agendas of the two trading partners by their powerful online industries. It calls upon governments, *inter alia*, not to "restrict the ability of suppliers to supply services over the Internet on a cross-border and technologically neutral basis". It also calls on governments not to restrict cross-border information flows or to require service suppliers in the ICT sector to use domestically located infrastructure or establish a local presence as a condition for them being permitted to operate. It also calls for certain due process guarantees and independence on the part of regulatory authorities (similar to the WTO Telecoms Reference Paper which requires an independent regulator).

The McKinsey report cited above noted that the most developed online ecosystems are in the US and the UK, with other countries such as Sweden quickly moving to consolidate their positions in this field. But with the EU, like the US, being a major exporter of these services, and with the Internet being arguably one of the most important platforms for the provision of services, it is no wonder that this issue has started to be taken up seriously in trade policy capitals like Brussels and Washington DC. The importance of this issue is only likely to grow as online markets become increasingly contested by emerging market providers from countries like India and China (although China still exports primarily goods rather than services) and Korea, which, as was noted above, is a world leader in broadband Internet penetration.

4. The USTR National Trade Estimate Report on Foreign Trade Barriers

The 2012 National Trade Estimate Report on Foreign Trade Barriers prepared and published by the United States Trade Representative (USTR)⁴⁰ also lists a number of countries and policies which fall within the scope of the Internet restrictions discussed here. In the section of the report that covers China, USTR has a long litany of complaints, bemoaning both the complexity of the Internet censorship regime and the unpredictability of its application.⁴¹ It also criticizes the restrictions on online audio and video distribution services⁴² as well as complaining more generally that "China has also yet to develop a legal framework conducive to the rapid growth of electronic commerce" noting that this is due, among other factors to "the paucity of credit card payment systems (exacerbated by a current monopoly provider of RMB denominated services)".⁴³ Other countries and trading partners also come in for criticism besides China in the USTR report. Other trade barriers USTR complains of include a "lengthy and onerous regulatory review" in Costa Rica, obstructing "a prospective supplier that has been seeking to provide Internet services via satellite",⁴⁴ as well as noting that in Egypt,

³⁹ See <http://www.ustr.gov/about-us/press-office/press-releases/2011/april/united-states-european-union-trade-principles-inform> (April 26, 2012).

⁴⁰ <http://www.ustr.gov/about-us/press-office/reports-and-publications/2012-1> (April 26, 2012).

⁴¹ USTR (2012), p. 85

⁴² Ibid, p. 86.

⁴³ Ibid, p. 96.

⁴⁴ Ibid, p. 113.

"one trade association has raised complaints since Egypt limits the provision of general Voice over Internet Protocol (VoIP) service to licensed wireline providers, effectively limiting the provision of VoIP services to its incumbent operator."⁴⁵ It also complains of restrictions related to data privacy regulation and legal liability for companies doing business over the Internet in the EU,⁴⁶ as well as barriers to Internet telephony in India.⁴⁷

The restrictions complained of in the 2012 report largely reflect those already brought up in the report of the preceding year, although the 2011 report had also complained of some Canadian restrictions on broadcasting which had impacted digital download services such as Netflix and which were part of Canada's policy of aggressively defending its own motion picture and audiovisual broadcasting industries and which seemed to have been resolved by the time the 2012 report was published. In sum, although most of the grievances expressed by USTR with regard to how countries regulate their online ecosystems relate to the prevalence of Internet piracy (reflecting the long-standing influence of interests such as the Motion Picture Association of America [MPAA] on US trade policy), it is also starting to sit up and take note of the massive economic losses (both real and potential) being incurred by US firms in overseas markets due to discriminatory and trade-inhibiting Internet restrictions, and this is slowly starting to manifest itself in corresponding language in its annual National Trade Estimate Report as discussed here.

As will be discussed in the next chapter, USTR is doing much more than catalogue these restrictions in an annual report, it has also decided to start conceptualizing and laying the groundwork for bringing and winning a case against one of the most economically significant offenders, China. In the next chapter, I examine how the existing trade rules we have as a result of the Uruguay Round of Multilateral Trade Negotiations can serve to counter the discriminatory and trade-restrictive effects of many of the measures complained of and discussed above.

⁴⁵ Ibid, p. 132.

⁴⁶ Ibid, p. 165.

⁴⁷ Ibid, p. 189.

IV. EXISTING TRADE RULES AND RESTRICTIONS OF INTERNET COMMERCE

1. The Most Important WTO Rules for Challenging Internet Restrictions

The fact that the body of multilateral trade rules we have now was largely negotiated between 1947 and 1993, a period when the Internet had either not been invented or had not yet been widely adopted by businesses and consumers, does not mean that these rules do not apply to Internet restrictions. One of the main achievements of the Uruguay Round was the negotiation of an agreement covering trade in services, the GATS. The approach taken to negotiating and scheduling binding liberalization commitments for services markets and adopting rules for their regulation was predicated on over 40 years of experience in the exchange of mutual tariff concessions and the negotiation of rules to stop governments from taking action that would reduce the value of these concessions. There was also a lot of work done during the 1970s in the GATT on non-tariff barriers that exerted their discriminatory and/or trade-restrictive effects behind the border, and this arguably provided a solid conceptual basis for crafting rules on the regulation of services markets, most of which also takes place behind the border. As shall be shown in the subsequent discussion, the historical pedigree that presaged the set of rules we now have in the form of the GATS is well suited to bringing and winning cases against behind the border regulation that unfairly discriminates against foreign service providers or is overly trade-restrictive. The potential application of WTO rules to Internet censorship and filtering has already been explored in the literature, most notably by Wu (2006) and by Hindley and Lee-Makiyama (2009). The analysis that follows builds on this work by examining the specific case now being prepared by USTR against China.

The most important trade rules for the purpose of the present discussion are arguably Article VI of the GATS on domestic regulation, Article XVI of the GATS on market access and Article XVII of the GATS on national treatment. Article III of the GATS on transparency also plays an important role as shall be seen in the next section which discusses the USTR's approach in a case currently being built against China. Although Article III obligations are enforceable in their own right, a lack of transparency is rarely on its own the commercial grievance that prompts a dispute, and complainants typically pair transparency claims with claims going to market access or competitive neutrality. I discuss each of these GATS Articles in turn before discussing both their respective implications for a potential case against China as well as what force they have been lent by the interpretative *acquis* of previous disputes where they were invoked.

Article VI of the GATS, entitled "Domestic Regulation" provides in paragraph 1 that "[in] sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner". This article also sets forth some fairly far-reaching constraints on administrative action as well as requiring that Members comply with a minimum set of institutional and due-process obligations in the context of administrative decisions affecting trade in services. Paragraphs 4 and 5 of Article VI require, inter alia, that, pending the entry into force of disciplines to be developed under paragraph 4, Members refrain from applying licensing and qualification requirements and technical standards that nullify or impair specific commitments in a manner that (a) is not based on objective and transparent criteria, (b) is more burdensome than necessary to ensure the quality of the service, or (c) in the case of licensing procedures, is in itself a restriction on the supply of the service. Importantly, however, Article VI:5(a)(ii) limits this obligation to measures that could not

reasonably have been expected of the Member concerned at the time its specific commitments were made. Since China's Internet filtering and licensing regime was already in place when it acceded to the WTO in December 2001, a claim under Article VI:5 would face a significant hurdle.

In the *US-Online Gambling* dispute, Antigua argued that the US had violated GATS Art. VI:1 "by failing to ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner", on the grounds that "it is impossible for foreign service suppliers to obtain authorization to supply services on a cross-border basis or even to apply for such an authorization", despite the fact that "exemptions from these laws had been granted to gambling operators of US origin, but not to foreign operators".⁴⁸ The Panel ultimately rejected Antigua's claims under this Article because it deemed that Antigua had failed to specify these claims beyond a set of vague allegations. However, in the context of its brief analysis of this claim, the Panel did provide some basic guidance on the substantive content of GATS Article VI. It noted that GATS Article VI "does not apply to measures of general application themselves but, rather, to the *administration* of these measures." It also stated that the language in Article VI:3 "imposes transparency and due process obligations with respect to the processing of applications for authorization to supply in a sector where specific commitments have been undertaken" and that Article VI:1 and VI:3 set forth disciplines of a "procedural nature".⁴⁹ I shall return to the implications of this language below.

Article XVI of the GATS is entitled "Market Access" and contains the key actionable disciplines that apply to WTO Members in how they regulate their services markets to allow access to foreign service suppliers. It requires Members to accord services and service suppliers of other WTO Members treatment no less favorable than that provided for under the terms, limitations and conditions agreed and specified in their services schedules (GATS Art. XVI:1). It also describes the kind of limitations and measures Members may not maintain against foreign service suppliers unless these are explicitly listed (reserved) on their schedules (GATS Art. XVI:2). These include (a) quantitative restrictions on the number of service suppliers allowed to operate in a given services sector, (b) upper value thresholds applicable to the service transactions or assets of a given services supplier, (c) limitation on the total number of service operations or quantity of service output, (d) a cap on the total number of natural persons that may be employed in a given service sector, (e) measures prescribing the legal form service suppliers must adopt (including joint ventures) in order to supply a service, and (f) foreign equity limits. These are of course precisely the kind of measures and limitations that WTO Members do typically inscribe on their schedules of specific commitments in services, but the value of this Article is that where they have failed to explicitly reserve the right in their schedules to impose such measures or limitations, they are prohibited from maintaining or adopting them. The list in Article XVI:2 is exhaustive, so that a measure falls foul of it only if it takes one of the listed forms. Crucially for present purposes, however, the Appellate Body held in the *US-Online Gambling* case that a measure prohibiting the supply of a service in respect of which a full market access commitment has been made amounts to a "zero quota" within the meaning of Article

⁴⁸ Report of the Panel in *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (WT/DS285/R), para. 6.427.

⁴⁹ *Ibid*, paras. 6.432-433.

XVI:2(a) and (c).⁵⁰ It is this reasoning that makes the wholesale blocking of a foreign service supplier's website potentially actionable under Article XVI.

Article XVII of the GATS is entitled "National Treatment". Like the national treatment obligation under GATT Art. III, the corresponding GATS obligation requires WTO Members not to treat foreign service suppliers any less favorably than domestic service suppliers with regard to all measures affecting the supply of services. The obligation contained in the GATS differs from its GATT counterpart in that WTO Members get to specify in their services schedules, on a sector-by-sector and mode-by-mode basis, any conditions and qualifications that will apply to the granting of such treatment. Finally GATS Art. XVII contains language in paragraph 3 which specifies that less favorable treatment shall be understood to mean treatment that "modifies the conditions of competition in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member."

2. The Case being built by USTR against China

On October 19, 2011, USTR issued a press release explaining that it was "seeking detailed information on the trade impact of Chinese policies that may block US companies' websites in China".⁵¹ The press release went on to elucidate that "a number of US businesses, especially small- and medium-sized enterprises, have expressed concerns regarding the adverse business impacts from periodic disruptions to the availability of their websites in China." Whether phrasing USTR's concerns in this language was really just to distract people from the fact that some of the US's biggest and savviest companies were the ones actually having the biggest problems with China and to make this action more politically palatable going into an election year is hard to fathom and largely beside the point. What this press release and the steps being taken announced by it implied, was that USTR had finally decided to take up the cause and start defending an area of economic activity where the US has an undeniable comparative advantage. In its press release, USTR announced that it had formally made a request for information subject to paragraph 4 of GATS Art. III, which imposes an obligation on Members to respond promptly to all requests by any other Member for specific information on any of its measures of general application which affect the operation of the GATS (i.e. that affect trade in services). Appended to the press release was the two and a half page letter sent by USTR to the Chinese government containing a detailed and expansive series of requests for information. The wording of these requests is very interesting, because it reveals the kind of tactical approach the US is contemplating as it prepares to bring a case against China for its hugely discriminatory and trade-distorting restrictions on Internet commerce.

Essentially, the requests ask the Chinese government to identify what ministries or government agencies are responsible for making and administering decisions on when to block a foreign website. It also asks what the guidelines are for this process and where they are published. It asks whether they are made public prior to being implemented. It also asks whether an affected service supplier can seek redress before the courts if its website is blocked, and whether the same procedures apply to foreign and domestic websites. In many ways, the questions being asked are slightly

⁵⁰ Appellate Body Report in United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services (WT/DS285/AB/R), paras. 238-252.

⁵¹ <http://www.ustr.gov/about-us/press-office/press-releases/2011/october/united-states-seeks-detailed-information-china%E2%80%99s-i>. (April 26, 2012).

disingenuous, because the US government is fully aware that there is almost certainly no process of prior public notice before guidance or regulations on blocking a website are implemented. Nor is there much hope that an affected foreign service supplier is able to seek effective redress in any kind of court or administrative proceedings. Finally USTR is fully aware that when policymakers in China adopt regulations and guidelines aimed at blocking websites, they approach this issue from a very different perspective for domestic firms than they do for foreign firms. This is firstly because of the different policy priorities it has towards the two sets of actors, but also because of the different instruments of control and coercion it has with respect to each. The chances that different procedures apply towards foreign and domestic firms are very high, and this is why USTR asked the question.

These shortcomings put China very much on the wrong side of GATS Art. III on transparency, particularly paragraph 1 which requires it to promptly publish any and all relevant measures of general application which affect trade in services. It also puts China very much on the wrong side of the language contained in GATS Art. VI on domestic regulation, which requires that where specific commitments have been undertaken, domestic regulation affecting these sectors be administered in a reasonable, objective and impartial manner. It is also very likely that given the nature of the relationship between the judiciary and the executive branches in China (the former is merely an extension of the latter's power), and the very under-developed and often ineffective nature of administrative review proceedings, that China will be on the wrong side of GATS Art. VI:2 (a), which requires WTO Members to maintain or institute arbitral or administrative tribunals or procedures which provide for the prompt review and appropriate remedies for administrative decisions affecting trade in services.

In short, the very secretive, opaque and arbitrary nature of how China's Internet censorship policies are administered, as documented by Google and various other sources, is very likely to see China fall far short of its transparency and domestic regulation obligations. Finally, if it can be shown that different procedures apply to foreign suppliers than to domestic suppliers, China is likely to find itself on the losing side of an argument alleging a national treatment violation. By asking these questions so directly, USTR is probably hoping that China will respond to its requests and inadvertently provide it with the proverbial "smoking gun", but it might also simply be a first shot over the bow, intended to convince China to simply stop directing its Internet censorship policies at US business interests who are in China pursuing solely commercial objectives.

3. The Importance of GATS Schedules and the Openness of Mode 1 Commitments

In addition to the transparency, domestic regulation and national treatment issues discussed above, China probably has a very big compliance problem with regard to just how open so many of its services sectors are under the most important mode of supply for Internet commerce, namely Mode 1, so-called "cross-border supply". A look at China's schedule of specific commitments in services shows that, like most countries that have joined the WTO after 1995 under the Article XII procedures⁵², China was asked to make relatively far-reaching commitments across the whole ambit of possible service sectors. Thus in a wide range of sectors, including legal services, accounting auditing and bookkeeping services, taxation services, medical and dental services, computer and

⁵² Meaning Article XII of the Marrakesh Agreement Establishing the WTO.

related services, software implementation services, real estate services, management consulting services, on and offshore oil-field services, photographic services, packaging services, convention services, translation and interpretation services, maintenance and repair services, courier services, audiovisual services, franchising services, wholesale or retail trade services away from a fixed location, all tourism and travel-related services, rail and road transport services, and freight forwarding agency services, China inscribed the word "none" under Mode 1, both in the market access and national treatment columns. The implication is that for foreign service suppliers providing their services in these sectors by means of the Internet, China is not able to impose any of the restrictions or measures listed in GATS Art. XVI unless such a restriction is covered by either one of the general or security exceptions (discussed in more detail in the next section).

Perhaps the more pertinent approach is to ask what services sectors China didn't make such an open commitment on, either by inscribing the word "unbound" under mode 1 in the market access and/or national treatment columns (meaning its freedom of action is generally unconstrained for this mode of supply and this services sector), or by inscribing a reference to its commitments under mode 3 (which involve commercial presence and which thus are generally formulated in more restrictive terms). This was the case for the following sectors: architecture (which only committed to no restrictions with regard to scheme design, otherwise cooperation with Chinese professional organizations was required in the market access column); advertising services (where registration and licensing requirements are scheduled); telecommunications services (which contains a reference to mode 3 for both value-added and basic telecommunication services); construction and related engineering services ("unbound"); distribution services ("unbound" for commission agents' and wholesale trade services, and "unbound except for mail order" for retailing services, an exception of obvious relevance to online retail); education services ("unbound"); environmental services ("unbound except for environmental consultation services"); financial services (mostly unbound); transport services (mostly unbound); computer reservation system services (requirements of a technological nature); and storage and warehousing services (unbound).

The implications of this kind of liberal market commitments and Internet commerce are huge, as was already laid out by the Panel in the *US-Online Gambling* case, when it considered the meaning of the word "None" when inscribed in the context of "mode 1". In this context the Panel reasoned that "mode 1 under the GATS encompasses all possible means of supplying services from the territory of one WTO Member into the territory of another WTO Member." and because of this "a market access commitment for mode 1 implies the right for other Members' suppliers to supply a service through all means of delivery, whether by mail, telephone, Internet etc., unless otherwise specified in a Member's Schedule." The upshot of this was that "a prohibition on one, several, or all means of delivery included in this mode 1 would be a limitation on market access for the mode" and that if a Member wishes to exclude market access with regard to the supply of a service through a given method of delivery covered by mode 1, then it must explicitly schedule such a limitation.⁵³ As was noted above, China has failed to schedule such a limitation under mode 1 in many of its services sectors, which ultimately means it will have to rely on being able to successfully invoke one of the exceptions allowed under the GATS in order to defend any such restrictions. As I discuss in the next section, however, these exceptions typically tend to get interpreted in a very narrow fashion, with

⁵³ Panel Report in *US-Online Gambling* cited *op. cit.*, paras. 6.288-290.

the burden being on the Member invoking them to adduce sufficient evidence that they are justified in a given instance.

4. The Narrowness with which GATS Exceptions are Interpreted

Article XIV of the GATS entitled "General Exceptions" sets out the scenarios and conditions subject to which Members may rely on this defense. It essentially provides that nothing in the GATS shall be construed to prevent any Member from taking any measures that are *inter alia* (a) necessary to protect public morals or to maintain public order (the latter only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society), (b) necessary to protect human, animal or plant life or health, and (c) necessary to secure compliance with laws or regulations that are not inconsistent with the GATS, including those intended to prevent fraud or to protect privacy. However, the real "hook" of GATS Art. XIV, and the language upon which most Members' efforts to invoke it ultimately founder is contained in the so-called *chapeau* of the Article, which provides any such measures taken by Member governments may not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail or a disguised restriction on trade. In addition, Article XIV bis provides a separate security exception, which has no equivalent chapeau and which China might seek to invoke, although the grounds it enumerates are narrow. The language of the general exceptions clause in GATS is of course very similar to the clause of the same name in the GATT⁵⁴, and panels have relied in the past, and will continue to rely in the future on the interpretative guidance that has been generated in previous disputes where the GATT exceptions clause was invoked. This was true in the *US-Online Gambling* case, where the Appellate Body referred to its interpretation of the "necessary" language in GATT Article XX(d) in the *Korea-Beef* case,⁵⁵ stating that "like the Panel, we find previous decisions under Article XX of the GATT 1994 relevant for our analysis under Article XIV of the GATS."⁵⁶

Panels and the Appellate Body have interpreted the scope and application of the *chapeau* in many disputes, and have essentially found it to place strict limits on the ability of Members to invoke the general exceptions. In *US-Shrimp*, the Appellate Body held "[in] our view, the language of the chapeau makes clear that each of the exceptions in paragraphs (a) to (j) of Article XX is a limited and conditional exception from the substantive obligations contained in the other provisions of the GATT 1994, that is to say, the ultimate availability of the exception is subject to the compliance by the invoking Member with the requirements of the chapeau."⁵⁷ The key in the context of Internet restrictions and overcoming a general exceptions defense will be to either challenge such restrictions on the basis of the "necessary" language, by demonstrating that the stated policy objectives being pursued by the Chinese authorities could have been achieved with a less trade-restrictive measure (this is what the US successfully argued in the *China-Publications and Audiovisual Products* case), as well as demonstrating that because China's Internet censorship practices subject foreign service suppliers to wholesale blocking, while Chinese suppliers of like services are permitted

⁵⁴ GATT Art. XX.

⁵⁵ Appellate Body Report in *US-Online Gambling* (WT/DS285/AB/R), para. 305, referring to the Appellate Body Report in *Korea - Various Measures on Beef* (WT/DS161/AB/R, WT/DS169/AB/R), para. 164.

⁵⁶ *Ibid*, para. 291.

⁵⁷ Appellate Body Report in *US-Shrimp*, para. 157.

to operate subject to self-censorship obligations, these practices amount in effect to unjustifiable discrimination between countries where like conditions prevail. This is likely to be the most contested element of any case, since China can point to the fact that domestic suppliers are also subject to its content controls.

5. *"China - Various Internet Restrictions" - Strength of a Potential US Case*

China's Internet restrictions seem to affect service suppliers across a wide range of scheduled service sectors. The strength of a specific dispute settlement action will inevitably depend on the openness of the sector in question in terms of China's mode 1 market access commitments. Such a case might not be strong in say, telecommunications services or banking, where China refrained from inscribing "none" on its schedule for mode 1 market access, but could be much stronger for, say "Wholesale or retail trade services away from a fixed location"⁵⁸ where China committed to unlimited market access and national treatment for mode 1. The difficulty is that the services most affected by China's Internet restrictions, such as search engines, social networks and video-sharing platforms, are most plausibly classified as value-added telecommunications or online information and database retrieval services, where China's mode 1 commitments refer back to its far more restrictive mode 3 commitments. The strength of a potential case is therefore likely to be inversely related to the commercial significance of the services concerned. Where Internet restrictions do impose limitations on the ability of service providers to compete on these markets, China can be challenged under the relevant GATS provisions on domestic regulation, market access and national treatment and any general exceptions defense it may seek to invoke would be likely to breach the strict confines set under the chapeau of GATS Art. XIV.

⁵⁸ This is section 4.E of China's Schedule of Specific Commitments, which covers direct selling and would arguably include providers such as Amway and Avon. Online retailers such as Amazon would more likely fall under retailing services (section 4.C), where China's mode 1 commitment is "unbound except for mail order".

V. THE NEXT GENERATION OF TRADE RULES ON INTERNET COMMERCE

1. The WTO Work Program on Electronic Commerce

In September 1998, the WTO General Council adopted a Work Program on Electronic Commerce in response to the Ministerial Declaration on Global E-Commerce that had formed part of the outcomes of the 2nd WTO Ministerial Meeting in Geneva earlier that year. The underlying rationale as one commentator explains, was a recognition that "the Internet offers unseen possibilities for digital trade and that offline trade barriers should not be replicated online."⁵⁹ The mandate of the Work Program was "to examine all trade-related issues relating to global electronic commerce, taking into account the economic, financial, and development needs of developing countries, and to report on the progress of the work programme, with any recommendations for action, to the Third Session (i.e. the Seattle Ministerial in 1999)." Electronic commerce also merited a mention in the Doha Ministerial Declaration of 2001, which acknowledged "electronic commerce creates new challenges and opportunities for trade for members at all stages of development, and we recognize the importance of creating and maintaining an environment which is favourable to the future development of electronic commerce."⁶⁰ Apart from emphasizing the desirability of reaching a consensus on what it terms the "trade treatment of electronically delivered software"⁶¹ and a provisionally agreed (albeit long-standing) practice of not imposing customs duties on electronic transmissions, it is hard to see what concrete results have been achieved from the Work Program to date. Clearly the growth of electronic commerce and the Internet in general has not been hindered by the inertia of the WTO Work Program.

The European Union and the United States have nevertheless chosen the Work Program (and by association the WTO) as a forum to advance a set of principles intended to "support the expansion of information and communication technology (ICT) networks and services, and enhance the development of electronic commerce."⁶² Referred to briefly above, these principles (entitled "Trade Principles for Information and Communication Technology Services") were put before the Work Program on Electronic Commerce in order to encourage WTO Members to embrace them and work to integrate them, "in a technologically neutral manner, into bilateral and multilateral trade disciplines".⁶³ The principles advocate *inter alia*: transparency; open networks, access and use; freedom of cross-border information flows; that governments refrain from imposing local infrastructure requirements on ICT service suppliers; full foreign participation in ICT services sectors; maximizing the availability and use of spectrum, ensuring that regulatory authorities are legally distinct and functionally independent from all service suppliers; and simplified authorization procedures that do not require legal establishment as a condition of supplying a service. In many ways, these principles are a logical extension to many of the principles already agreed on during the Uruguay Round overtime negotiations on telecommunications services, as manifested in the

⁵⁹ Wunsch-Vincent (2008) p. 1.

⁶⁰ Para. 34.

⁶¹ WTO, Work Program on Electronic Commerce, Decision of 2 December 2009 (WT/L/782) circulated on 11 December 2009.

⁶² WTO, Communication from the European Union and the United States Contribution to the Work Programme on Electronic Commerce (S/C/W/338) circulated 13 July 2011.

⁶³ *Ibid*, p. 2.

Telecoms Reference Paper. But in other ways these principles seek to enshrine the openness of the Internet and ICT services as a universally accepted principle of international commerce and to remove these issues somewhat from the human rights aspects that have tinged much of the debate about freedom and the Internet, and which governments in countries that are not liberal democracies (including China) are openly hostile towards.

These Principles were only brought before the WTO Council for Trade in Services in July of 2011, shortly before the August summer hiatus, and it is as yet unclear what kind of impact they will have and whether they will be actively taken up and adopted as a basis for some kind of future binding treaty text. This is admittedly very unlikely in the context of the present Round, where the issues up for negotiation were defined long ago and where, following the Eighth Ministerial Conference in December 2011, Members have acknowledged that the negotiations are at an impasse. Given that the most recent phases of active negotiation in the Doha Round had focused on narrowing differences in existing negotiating texts and on the modalities for tariff reductions in agricultural and non-agricultural trade, it seems unlikely that it would be possible to get 155 Members to agree to take up negotiations on a set of principles intended to govern freedom of commerce over the Internet. These are thus rules that will likely have to wait for the next Round of trade negotiations.

2. The Trans Pacific Partnership

To make the wait a little easier, governments in countries that have a strong commercial interest in promoting freedom of access to information and communications networks and services are also negotiating with each other directly, in the form of preferential trade agreements covering a range of so-called new issues that are not currently part of multilateral trade negotiations at the WTO. One forum where this is going on very actively, and in a way that will likely define the future shape of multilateral commitments in this area (should they ever be agreed), is under the auspices of the Trans-Pacific Partnership (TPP), currently being negotiated between Brunei Darussalam, Chile, New Zealand and Singapore (already members of the Trans-Pacific Strategic Economic Partnership Agreement (P4)), with Australia, Peru, the USA, Vietnam and Malaysia. Japan, Canada and Mexico have also expressed a strong interest in joining the negotiations.

In November 2011, and very much in the context of the ongoing TPP negotiations and following USTR's request for information from China, the National Foreign Trade Council (NFTC) released a set of US business community policy priorities for modernizing the international trade rules and practices governing cross-border flows of data and information technologies, calling for the US government to *inter alia* seek commitments that would: expressly prohibit restrictions on legitimate cross-border information flows; prohibit local infrastructure or investment mandates; promote international standards, dialogues and best practices, improve transparency and predictability, and address legal and policy issues involving the digital economy.⁶⁴ When issuing the policy document the NFTC noted that

⁶⁴ National Foreign Trade Council "Promoting Cross-Border Data Flows. Priorities for the Business Community" available at <http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf> (April 26, 2012).

"The policy priorities were developed by a core group of associations and companies through a process convened under the National Foreign Trade Council. A variety of America's leading companies including Citi, Google, IBM, Mastercard, Microsoft and Visa joined NFTC and other associations including the Business Software Alliance, Coalition of Services Industries, Software & Information Industry Association and U.S. Council for International Business to craft the document."⁶⁵

In the context of the TPP negotiations specifically, USTR has submitted two proposals on the issue of the free flow of data over the Internet. The first proposal (tabled in June 2011 during the seventh round of TPP talks) would commit TPP countries to refrain from blocking cross-border transfers of data. The second proposal (tabled during the ninth round of TPP negotiations in Peru in October 2011) would bar countries from putting in place requirements that a company store all of its data for local use on a server located in-country, but this approach seems rather piece-meal given the relevant US industry's widely held convictions that a more comprehensive body of rules is what's needed.

The broad framework of the TPP Agreement that was released by the USTR last November⁶⁶ addresses the kind of Internet restriction discussed in this paper under a number of headings. These include "Cross-Border Services", where TPP countries are working towards consensus on "securing fair, open, and transparent markets for services trade, including services supplied electronically and by small- and medium-sized enterprises, while preserving the right of governments to regulate in the public interest."⁶⁷ Another issue area where this is addressed is "E-Commerce", where the USTR release claims that "[n]egotiators have made encouraging progress, including on provisions addressing customs duties in the digital environment, authentication of electronic transactions, and consumer protection. Additional proposals on information flows and treatment of digital products are under discussion."⁶⁸ Finally, TPP negotiators are said to also be working on a text covering telecommunications, which is said to address "the need for reasonable network access for suppliers through interconnection and access to physical facilities".

In sum, it is probably safe to say that the body of rules and the set of commitments that emerge from the TPP process will push the boundaries beyond the largely implicit set of rights and obligations relating to the digital and online economy contained in the WTO texts following the Uruguay Round and will pave the way and set the bar for the incorporation of more explicit guarantees in future multilateral rules. This is something that is also going on in the OECD, which is discussed immediately below.

⁶⁵ See <http://www.nftc.org/newsflash/newsflash.asp?Mode=View&id=236&articleid=3356&category=All> (April 26, 2012).

⁶⁶ See http://insidetrade.com/iwpfile.html?file=nov2011%2Fwto2011_4129b.pdf (April 26, 2012).

⁶⁷ Ibid.

⁶⁸ Ibid.

3. The OECD Framework

Research and policy dialogue concerning various aspects of the Internet have been going on in the OECD for over three decades. Starting out largely from the perspective of privacy concerns,⁶⁹ this work now encompasses many different aspects of the Internet economy. More recently, this work has been guided by the 2008 Seoul Declaration for the Future of the Internet Economy⁷⁰ which laid the foundation for working towards a consensus on the adoption of shared principles for an open Internet economy, primarily through the exchange of best practices in four key areas of, namely (1) supply, (2) demand, (3) measurement, and (4) principles for an open internet.⁷¹ Only the last of these four aspects concerns the focus taken in this paper. A 2011 High Level Meeting on the Internet Economy which took place from the 28-29 June 2011, issued a final communiqué⁷² containing a set of "basic principles for Internet policy-making" which included, for our purposes, the following: promoting and protecting the global free flow of information; promoting the open, distributed and interconnected nature of the Internet; promoting and enabling the cross-border delivery of services; ensuring transparency, fair process, and accountability.

It seems that policymakers and regulators, at least in a limited number of developed country capitals, are coalescing around a core set of principles advocating for transparency, openness and due process in the administration of Internet regulatory regimes. This is happening within the framework of the Transatlantic Economic Council, the WTO Work Program on Electronic Commerce, the OECD, as well as in other *fora* that have not been discussed here due to space limitations.⁷³ It seems a foregone conclusion that sooner or later these principles will find themselves explicitly set forth in binding multilateral trade disciplines, unless of course some developing countries and emerging economies maintain the kind of resistance they have shown for over a decade now to negotiating issues such as trade and the environment, trade and labor issues, trade and competition and trade and investment.⁷⁴

4. Possible Pushback from Some Developing Countries and Emerging Economies

In many ways it is not completely accurate to portray initiatives to strengthen open Internet commerce by some countries and efforts to unilaterally impose restrictions on Internet commerce by others as a purely "North-South" issue. There seems to be a general recognition by all

⁶⁹ The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data date from 1980; see also the OECD Declaration on Transborder Data Flows dated April 11, 1985, available at http://www.oecd.org/document/60/0,3343,en_2649_34225_2373500_1_1_1_1,00.html (April 26, 2012).

⁷⁰ See <http://www.oecd.org/dataoecd/49/28/40839436.pdf> (April 26, 2012).

⁷¹ See http://www.oecd.org/document/13/0,3746,en_21571361_47081080_47086157_1_1_1_1,00.html (April 26, 2012).

⁷² See <http://www.oecd.org/dataoecd/40/21/48289796.pdf> (April 26, 2012).

⁷³ APEC is another forum where these issues have been actively taken up, see for example the APEC Principles for Cross-Border Trade in Services, available at <http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Group-on-Services> (April 26, 2012).

⁷⁴ These issues have all been "non starters" at the WTO at various times since the Organization's establishment in 1995, with the result being that instead of being negotiated in a relatively open and transparent forum like the WTO, where consensus-based decision-making imposes some sort of counter-balancing force to market power, rules on most of these issues have now been negotiated in bilateral or regional arrangements where the dynamics of market power are relatively unconstrained.

stakeholders, developed and developing, that the Internet and related ICT networks and services can be a transformative engine of growth. Developed countries like the US, with its global dominance in online search engines or social networking sites, as well as developing countries like India, which has reaped huge benefits from the IT revolution and the cross-border supply of software services and back-office support services, realize that an open Internet is good for everyone, even if developed countries are positioned to benefit the most from the continuation of these policies. The difficulty comes in convincing developing countries that advancing and adopting principles on an open Internet should be higher up on the list of policy priorities than other urgent focuses for collective action, like alleviating global poverty, eradicating diseases that kill millions of people in developing countries, or removing trade-distorting subsidies and market access barriers on products that developing countries have a comparative advantage in, like, say agricultural commodities. Clearly, if a small subset of developed countries want to achieve rapid and real progress on multilateral rules and principles to keep the Internet open and data flowing freely across borders, it will probably be necessary to trade this desired outcome off against something tangible and genuinely useful for developing countries. At least that would be a way to put this issue somewhere near the top of the agenda.

Middle income developing countries and emerging economies are a much harder proposition, because in these countries having governments agree to the kind of principles those who advocate for freedom of Internet commerce aspire to, is predicated on a much more complex political-economy calculus, which pits the development priorities of leaders and the vested interests of market incumbents against the "freedom" that those who would enter these markets are claiming as their own. As was done in the GATS negotiations during and immediately after the Uruguay Round, this is probably best done by the request and offer process inherent to services negotiations, subject to a now (broadly accepted) understanding that mode 1 also includes trade in services over the Internet.

VI. FINDINGS AND CONCLUSIONS

There have already been a number of WTO cases either directly involving or tangentially related to the cross-border supply of services over the Internet. It seems to be well understood that mode 1 market access and national treatment commitments cover services supplied over the Internet. In some ways, the United States' "loss" in the Online Gambling case has arguably paved the way for the US to mount its own challenge against the broad array of Internet restrictions perpetrated by China against foreign service suppliers and economic operators. This is what I believe is now going on behind USTR's request for information from China under GATS Art. III last October. I also believe, based on the (admittedly somewhat brief) reasoning provided above, that the US would stand a reasonable chance of prevailing on this issue at the WTO, at least in those sectors where China has made full mode 1 commitments, although the extent to which this would achieve a wide-ranging and profound rethink of China's Internet policies by the Chinese leadership is of course highly questionable. The Chinese government's Internet policies are shaped above all by the Chinese Communist Party's priority of maintaining political stability and its own hold on power. Whatever changes the US succeeds in bringing about for foreign commercial operators in terms of Internet restrictions will be constrained by the Communist Party's perceptions on how compatible such changes are with its own priorities. The same is of course broadly true in any country, to the extent that a "win" at the WTO only translates into a genuine change in the domestic policies of the "losing" party to the extent this is politically expedient and palatable to it. To find proof of this, one need look no further than to the "winners" of the *US-Online Gambling* case, Antigua and Barbuda.

REFERENCES

1. Abbate, Janet. "Government, Business and the Making of the Internet." *The Business History Review*, 2001: 147-176.
2. Barboza, David. "Mining Executive Held by China Is Seen as an Unlikely Pawn." *The New York Times*. July 26, 2009. <http://www.nytimes.com/2009/07/27/world/asia/27riotinto.html> (accessed April 26, 2012).
3. BBC. "Sopa and Pipa anti-piracy bills controversy explained." *BBC News Technology*. January 17, 2012. <http://www.bbc.com/news/technology-16596577> (accessed April 27, 2012).
4. Bennetto, Jason, and Terri Judd. "Glitter collected pictures of girls being abused children." *The Independent*. November 13, 1999. <http://www.independent.co.uk/news/glitter-collected-pictures-of-girls-being-abused-children-1125566.html> (accessed April 27, 2012).
5. Chang, Andrea, and Jim Puzzanghera. "Apple, e-book publishers accused of price fixing." *Los Angeles Times*. April 11, 2012. <http://www.latimes.com/business/la-fi-apple-antitrust-20120412,0,6850297.story> (accessed April 26, 2012).
6. Eriksson, Johan, and Giampiero Giacomello. "Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State." *International Studies Review*, 2009: 205-230.
7. Federal Communications Commission. *Connecting America: The National Broadband Plan*. Washington DC: Government Printing Office, 2010.
8. George-Cosh, David. "Regulator loosens grip on Skype ban." *The National*. January 10, 2011. <http://www.thenational.ae/business/technology/regulator-loosens-grip-on-skype-ban> (accessed April 2, 2012).
9. Google. "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information." 2010.
10. Halliday, Josh, and Charles Arthur. "WikiLeaks fights to stay online after US company withdraws domain name." *The Guardian*. December 3, 2010. <http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns> (accessed April 26, 2012).
11. Hansen, Kristena. "Google's data collecting is subject of multi-state investigation." *Los Angeles Times*. June 22, 2010. <http://articles.latimes.com/2010/jun/22/business/la-fi-google-20100622> (accessed April 26, 2012).
12. Hindley, Brian, and Hosuk Lee-Makiyama. *Protectionism Online: Internet Censorship and International Trade Law*. ECIPE Working Paper No. 12/2009. Brussels: European Centre for International Political Economy, 2009.

13. Kelty, Christopher. "The disappearing virtual library." *Aljazeera*. March 1, 2012.
<http://www.aljazeera.com/indepth/opinion/2012/02/2012227143813304790.html>
(accessed April 27, 2012).
14. McGregor, James. *One Billion Customers: Lessons from the Front Lines of Doing Business in China*. Free Press, 2005.
15. McGregor, Richard. *The Party*. Harper Collins, 2010.
16. McKinsey Global Institute. *Internet matters: The Net's sweeping impact on growth, jobs and prosperity*. McKinsey & Company, 2011.
17. Meller, Paul. "Europe Moving Toward Ban On Internet Hate Speech." *The New York Times*. November 10, 2001. <http://www.nytimes.com/2001/11/10/business/international-business-europe-moving-toward-ban-on-internet-hate-speech.html> (accessed April 26, 2012).
18. Organization for Economic Cooperation and Development. *Regulatory Policy: Towards a New Agenda Pathways to the Future*. Conference Proceedings, Paris: OECD, 2010.
19. Palfrey, John G. *Local Nets on a Global Network: Filtering and the Internet Governance Problem*. Public Law & Legal Theory Working Paper Series, Harvard Law School, 2010.
20. Peltzman, Sam. *Toward a More General Theory of Regulation*. NBER Working Paper No. 133, NBER, 1976.
21. Purkayastha, Debapratim, and Hadiya Faheem. *eBay's Problems in China*. Case study. Hyderabad: IBS Center for Management Research, 2008.
22. United States Trade Representative. *2012 National Trade Estimate Report on Foreign Trade Barriers*. Washington DC: Office of the United States Trade Representative, 2012.
23. Virzi, Anna Maria. "Hate Or History?" *Forbes*. July 3, 2001.
<http://www.forbes.com/2001/07/03/0703wwllmem.html> (accessed April 26, 2012).
24. Wu, Tim. "The World Trade Law of Censorship and Internet Filtering." *Chicago Journal of International Law*, 2006: 263-287.
25. Wu, Tim, and Jack Goldsmith. *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press, 2006.
26. Wunsch-Vincent, Sacha. "Trade rules for the digital age." In *GATS and the Regulation of International Trade in Services*, edited by Marion Panizzon, Nicole Pohl and Pierre Sauvé, 497-529. Cambridge University Press, 2008.