UIC John Marshall Journal of Information Technology & Privacy Law

Volume 28
Issue 2 *Journal of Computer & Information Law - Winter 2010*

Article 4

Winter 2010

Internet Filtering: The Ineffectiveness of WTO Remedies and the Availability of Alternative Tort Remedies, 28 J. Marshall J. Computer & Info. L. 273 (2010)

Kristen A. Knapp

INTERNET FILTERING: THE INEFFECTIVENESS OF WTO REMEDIES AND THE AVAILABILITY OF ALTERNATIVE TORT REMEDIES

KRISTEN A. KNAPP*

I. INTRODUCTION

In recent years, Internet filtering, while not a new phenomenon, has grown both in the United States and across the globe.[1] Empirical studies by organizations such as OpenNet Initiative show the pervasiveness of government filtering is increasing worldwide.[2] Governments are no longer the only actors conducting Internet filtering. Increasingly, private actors, such as Internet Service Providers ("ISPs"), have taken on filtering responsibilities that require them to act in a quasi-governmental capacity, prompting questions of whether these entities are really private actors or actually agents of the state.[3] Internet filtering will only continue to increase in importance as more nations undertake Internet filtering and technology improves to facilitate easier and more effective filtering.[4]

As a result of these developments, commentators have recently begun to speculate, after the decision by the World Trade Organization ("WTO") in *United States – Measures Affecting the Cross-Border Supply*

* J.D., *Cum Laude*, Northwestern University School of Law, 2010; B.A., Wesleyan University, 2005. I am extremely grateful to Professor Jim Speta for his guidance and advice during the research and writing process and special thanks to Kevin King for his encouragement and support.

1. Jonathan Zittrain & John Palfrey, *Introduction*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 1, 2 (Ronald Diebert, et al. eds., 2008) (noting that "[m]ore than three dozen states around the world now filter the Internet").

2. Mary Rundle & Malcolm Birding, *Filtering and the International System: A Question of Commitment*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 73, 90 (Ronald Diebert, et al. eds., 2008).

3. *Id.* at 76.

4. John G. Palfrey, *Preface*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING ix, ix (Ronald Diebert, et al. eds., 2008).

of Gambling and Betting Services,[5] whether some Internet filtering might violate WTO commitments under the General Agreement on Trade in Services ("GATS Agreement").[6] Professor Tim Wu has argued that China would struggle to justify its restrictive Internet filtering practices under the GATS Agreement.[7] China, like the U.S., has made quite extensive commitments to liberalize services including "data processing services."[8] The most likely Internet-based services that fall within the scope of data processing services are search engines. As Wu argues, China's Internet filtering in the past has included the outright blocking of foreign search engines, *e.g.*, the 2002 seizure of Google.com, which likely violated China's WTO commitments or at the very least raises substantial questions about the legality of such actions.[9] Furthermore, Wu raises significant questions about China's ability to justify its filtering under the commonly cited exception to the GATS Agreement: protection of public morals and maintenance of public order.[10] To justify blocking foreign search engines, China would be forced to argue that such actions were necessary to maintain political control within China, in essence attempting to justify a protectionist measure on the basis of its need to ensure political suppression of dissident views.[11]

Additionally, in late 2009, the European Centre for International Political Economy ("ECIPE") published an extensive study on the state of Internet censorship and the applicability of international trade law to Internet filtering. Similarly to Wu, the ECIPE study concluded that China, among other countries such as Mexico and Germany, who all participate in blocking VoIP services, would struggle to justify its current

5. Appellate Body Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R (Apr. 7, 2005) [hereinafter U.S. – Gambling Services Appellate Body Report]; Panel Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R (Nov. 10, 2004) [hereinafter U.S. – Gambling Services Panel Report].

6. *See* Tim Wu, *Legal Implications of a Rising China: The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J. INT'L L. 263 (2006); Brian Hindley, & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law*, (European Ctr. For Int'l Political Econ., Working Paper No. 12/2009, 2009), *available at* http://www.ecipe.org/publications/ecipe-working-papers/protectionism-online-internet-censorship-and-international-trade-law/PDF.

7. Wu, *supra* note 6, at 265.

8. *Id.* at 281.

9. *Id.* at 283-4.

10. General Agreement on Trade in Services art. XIV(a), Apr. 15, 1994, 1869 U.N.T.S. 183 [hereinafter GATS Agreement].

11. Wu, *supra* note 6, at 284 (". . .WTO panels and Appellate Bodies face the unappetizing prospect of trying to decide when a given part of China's system of information control represents a measure that combats 'a genuine and sufficiently serious threat' that affects 'one of the fundamental interests of society.'").

filtering efforts in light of its GATS Agreement commitments.[12] Thus, it seems clear, or as clear as it can be without an actual WTO case testing these propositions, that the practices of some nations, particularly China, fall within the scope of the GATS Agreement and represent violations of the Agreement.

Other commentators, however, argue that the WTO legal agreements that would likely govern any future Internet filtering case are incomplete and ill-suited to the task.[13] The "GATS is an incomplete system. It requires new negotiations to extend it to newer sectors" and these negotiations have not been entirely forthcoming.[14] Moreover, real concerns remain regarding the ability of the WTO to interpret the GATS Agreement, an Agreement drafted when the Internet was in its infancy, in a consistent and meaningful manner given the extensive technological change that has taken place since the mid-90s.[15] Hence, companies doing business on the Internet negatively affected by Internet filtering practices may be better served by looking beyond the WTO's dispute settlement mechanism, to common law tort doctrines for legal remedies.

Recent technological innovations, particularly a change in the types of devices accessing the Internet, will make Internet regulation and consequently filtering easier to accomplish in the future. One commentator has described this evolution as the "appliancization" of the Internet.[16] Historically, people accessed the Internet using "generative" devices, but increasingly, in part because of technological innovation and in part because of consumer demand, people are accessing the Internet with "sterile" devices that are tethered.[17] Generative technologies invite tinkering and innovation, *e.g.,* the PC that can be programmed and reprogrammed by the user; while sterile technologies come preprogrammed and cannot be reprogrammed by the user, *e.g.,* cell phones.[18] The nature of the endpoint matters because the more easily a third-party can regulate the

12. Hindley & Lee-Makiyama, *supra* note 6.

13. *See* Stuart S. Malawer, *Internet Commerce and Trade Policy*, VA. LAW. 2 (1999), http://www.worldtradelaw.net/articles/malawerinternettrade.pdf.

14. *Id.* at 4.

15. *See e.g.,* Nancy J. King & Kishani Kalupahana, *Choosing Between Liberalization and Regulatory Autonomy under GATS: Implications of U.S. – Gambling for Trade in Cross Border E-Services*, 40 VAND. J. TRANSNAT'L L. 1189, 1198 (2007) (noting ". . .U.S. – Gambling also reinforces the uncertainties of a relatively undeveloped GATS legal framework.").

16. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 8 (2008) ("This counterrevolution would push mainstream users away from a generative Internet that fosters innovation and disruption, to an appliancized network that incorporates some of the most powerful features of today's Internet while greatly limiting its innovative capacity – and, for better or worse, heightening its regulability.").

17. *Id.* at 3-8.

18. *Id*. at 3.

endpoint the more easily that third-party can filter the Internet.[19]

The more the Internet becomes appliancized with tethered appliances the more easily third-parties will be able to filter users' access to the Internet. Internet filtering is often thought of as merely technical filtering, or in other words blocking or removing content from websites, but its definition need not be so narrow. Internet filtering includes any means of limiting access to the Internet.[20] Hence, part of the risk posed by the appliancization of the Internet is the new ability to "filter" the Internet by reprogramming the sterile devices at the endpoints that individuals use to access the Internet, at a time when those individuals have no ability to prevent or undue such reprogramming.[21]

Appliancization of the Internet contributes to the ease with which code functions as law because "the software we use shapes and channels our online behavior as surely as – or even more surely and subtly than – law itself."[22] As Jonathan Zittrain has noted, "[j]ust as technology's functionality defines the universe in which people can operate, it also defines the range of regulatory options reasonably available to a sovereign"[23] and arguably the breadth of mechanisms available for Internet filtering.

Beyond advances in technology, a change in consumer tastes has also contributed to the appliancization of the Internet. First, greater numbers of unsophisticated users began using the Internet as the level of Internet penetration increased and with these unsophisticated users came increasing fears of insecurity on the Internet.[24] The solution was to make the means of accessing the Internet less generative and thus less susceptible to user error.[25] Furthermore, the amount of content on the Internet has increased considerably since the birth of the Internet and the rate at which new content is produced is starting to have detri-

---

19. For an early example of Internet filtering at the endpoints consider *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 26, 1995), where Prodigy, an early ISP was held liable for failing to remove defamatory content posted on one of its bulletin boards when Prodigy had held itself out to be actively monitoring and filtering the content of its bulletin boards.

20. Palfrey, *supra* note 4, at ix.

21. ZITTRAIN, *supra* note 16, at 104. For a very recent example, consider the action by Amazon of removing the George Orwell novels *1984* and *Animal Farm* from Kindle users' Kindles without permission or prior notification. *See* Brad Stone, *Amazon Erases Orwell Books From Kindle*, N.Y. TIMES, July 17, 2009, http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

22. ZITTRAIN, *supra* note 16, at 104 (agreeing with Lessig and Reidenberg's theory that code can be law and applying it to the context of Internet filtering).

23. *Id.* at 105.

24. *Id*. at 58.

25. *Id.* at 59 (noting that this was a particularly common solution in places where the user did not own the computer, such as schools, offices, libraries and cybercafés).

mental effects on other aspects of the Internet.[26] To make that content useful to the new generation of Internet consumers it has become imperative to organize the content.[27] Consumers have demanded increased information on the Internet and the more organized consumers demand the Internet become, the easier it will be for governments or private actors to filter the Internet.[28]

Second, the rise of Web 2.0 – although seemingly generative because the user is given considerable ability to determine function, content, and appearance – is part of the movement toward the appliancization of the Internet.[29] Web 2.0 refers to the time period since approximately 2004, during which web applications have become increasingly geared toward interactive content and harnessing the collective creative abilities of Internet users. Web 2.0 content can be created and edited directly by users, through sites such as social networking sites, video and picture sharing sites, blogs, and wikis.[30] However, Web 2.0 programs are not truly generative because, although they facilitate the creation of user-generated content, just as with a common kitchen blender, the user's options to customize that content are limited. Your kitchen blender might be able to crush ice to make margaritas, but it cannot julienne potatoes for the family dinner. Similarly, a blog might allow for a range of content layouts and a text comment function, but if you want to allow video comments you are not going to be able to use that blog service. Hence, most Web 2.0 software is nothing more than a dumb appliance that the user does not have the ability to reprogram to suit the user's individual preferences.

This paper addresses two possible legal responses to the rise of Internet filtering. First, the paper argues that U.S. Internet filtering practices generally do not violate U.S. GATS commitments. Rather, the WTO's decision in *U.S.-Gambling Services* was unique and unlikely to be repeated because (1) the U.S. is predominately an exporter of electronic services and not an importer, and (2) the *U.S.-Gambling Services* decision resulted from a denial of market access. Instead, those seeking to

26. Martin Peers, *Future Shock for Internet Ads?*, WALL ST. J., Feb. 17, 2009, at C10, *available at* http://online.wsj.com/article/SB123483323444195983.html (pointing to the "explosion of user-generated content" as partly responsible for declining ad revenues).

27. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 51 (2006) (highlighting the fact that information wants to be grouped, labeled, and otherwise sorted).

28. *Id.*

29. ZITTRAIN, *supra* note 16, at 102.

30. Tim O'Reilly & John Battelle, *Web Squared: Web 2.0 Five Years On*, WEB 2.0 SUMMIT, (2009), http://assets.en.oreilly.com/1/event/28/web2009_websquared-whitepaper.pdf (noting Tim O'Reilly coined the term Web 2.0 in a conference in 2004, unsurprisingly titled Web 2.0 Conference).

impose legal liability for U.S. filtering practices should pursue tort remedies, specifically for tortious interference in contractual relations.

Part II provides technical background on how Internet filtering is accomplished in practice, including the range of types and methods of Internet filtering. It also explores how the actors responsible for Internet filters are shifting. Part III details the GATS Agreement that was held to govern Internet filtering in the *U.S.-Gambling Services* decision and would likely govern other filtering actions, including both the exceptions to this regime and why the *U.S.-Gambling Services* decision is unlikely to affect future U.S. filtering efforts. In Part IV the paper surveys the current range of U.S. Internet filtering actions and why these actions are unlikely to violate WTO GATS commitments.

Part V details how tort remedies, such as those available for the intentional interference in contractual relations and at-will relationships are likely to be better legal remedies than WTO law for companies affected by U.S. Internet filtering actions. Although there are only a limited number of cases that have applied the tort of intentional interference in contractual relations in the Internet context, those precedents suggest plaintiffs can recover provided they establish that the filtering was both intentional and improper.[31] The outlook is similarly positive for at-will relationships, which require proof of similar elements as contractual relationships.[32] Part VI briefly concludes.

II. HOW DO GOVERNMENTS AND PRIVATE ACTORS FILTER THE INTERNET?

Internet filtering is not simply the blocking of content by the government or a private actor; Internet filtering encompasses content restrictions as well as licensing requirements, legal liability regimes, registration requirements, and methods that promote self-monitoring by Internet users.[33] Nor is Internet filtering uniform in terms of the manner in which it is conducted or the location at which it takes place in the Internet's physical architecture. The kind of Internet filtering attempted varies with the motivations of the filtering group and the group's capabilities and resources available to conduct Internet filtering.[34] The actors responsible for Internet filtering have also begun to change.

31. RESTATEMENT (SECOND) OF TORTS §766 (1979).

32. *See* Vulcan Golf, LLC v. Google, Inc., 552 F. Supp. 2d 752 (N.D. Ill. 2008) (denying defendant's motion to dismiss).

33. Jonathan Zittrain & John Palfrey, *The Politics & Mechanisms of Control*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 29, 32-33 (Ronald Diebert, et al. eds., 2008).

34. Steven J. Murdock & Ross Anderson, *Tools and Technology of Internet Filtering*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 57, 58-59 (Ronald Diebert et al. eds., 2008).

Governments are increasingly relying on private actors, such as ISPs and other intermediaries, to conduct Internet filtering, complicating the imposition of liability on those actors.

A. Physical Architecture of the Internet

The Internet relies on a physical architecture to deliver content to users. That architecture is comprised of several pieces. At one end there is the user at a computer or, as is often the case now, a cell phone, iTouch, iPad, or eBook reader. Second, the inner workings of the Internet control the user's ability to access content. The inner workings can be divided into two parts: (1) DNS servers and (2) routers. Internet filtering can take place at both the DNS server location and at the router location.

The DNS server allows the user, who has typed in a domain name or URL, such as www.google.com, to find the IP address for that domain name. Once the IP address is determined, the user's computer, connecting via a router, is able to find the computer on the Internet that hosts the desired website.[35] The router's job is particularly important and more commonly the locus of Internet filtering efforts than at the DNS server phase.[36] The router receives information, called packets, from both the user's computer and information located on other computers on the Internet and determines how to send the information to its destination.[37] Once the router directs the information, the requested web page is loaded on the user's Internet device allowing the user to view it.[38] The packets that the router receives are uniform to the extent that they all rely on the TCP/IP protocol to encode the information they contain, thus explaining how the different routers on the Internet are able to communicate with one another.[39]

B. Types of Filtering

Content filtering operates by disrupting the physical architecture of the Internet at some phase in the transmission of either (1) the request to locate the IP address or (2) the process of loading the website onto the

35. *Id*. at 57-58.

36. Jonathan Zittrain, *Internet Points of Control,* 44 B.C. L. Rev. 653, 658 (2003) ("Routing is critical because the phase at which control is attempted is one of the most important factors contributing to a given control strategy's strengths and shortcomings as matters of both engineering and policy."). *See also* Robert E. Kahn and Vinton G. Cerf, *What is the Internet (And What Makes it Work)?* (Dec. 1999), http://www.policyscience.net/cerf.pdf (describing routers as a "key architectural construct").

37. Murdock & Anderson, *supra* note 34, at 57.

38. *Id*. at 57-58.

39. *Id*. at 57.

user's Internet device so the user can view the website.[40] An in depth discussion of the technical methods of carrying out content filtering is beyond the scope of this paper, but it is important to highlight the difference between three kinds of content filtering: DNS tampering, TCP/IP header filtering, and TCP/IP content filtering.

DNS tampering occurs during a request to locate an IP address. Typically it works by giving the ISP's DNS server a list of blocked IP addresses. When the user's computer requests the blocked IP address an erroneous answer or no answer is returned.[41] TCP/IP header filtering operates by looking at the IP address information contained in each packet of information. Using a block list,[42] a router can be configured to drop packets headed to IP addresses on the block list.[43] In contrast to TCP/IP header filtering, TCP/IP content filtering is more invasive and more likely to be accurate. TCP/IP content filtering involves inspecting the actual content of the packet, rather than just its address information, to determine whether the content contains banned keywords.[44] This kind of filtering, while being even more accurate, has the drawback of potentially being more expensive as additional equipment may be necessary.[45]

Licensing requirements, although seemingly neutral, may be an increasingly popular means of filtering, especially if one believes Zittrain's "appliancization" of the Internet argument. Licensing requirements target the Internet's growing cadre of intermediaries and require them to carry out Internet filtering.[46] The most studied licensing requirement in the U.S. that imposes Internet filtering requirements is the Federal Communication Commission's ("FCC") implementation of the Children's Internet Protection Act ("CIPA").[47] CIPA requires schools and libraries wishing to receive discounts offered by the E-rate program to certify that they have an "Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene, (b) child pornography, or (c) harmful to minors (for computers that are accessed by minors)."[48]

Even in the absence of a licensing requirement, the government can

40. *Id*. at 57-58.

41. *Id*. at 60-61

42. Block lists are discussed *infra* in Section IIB.

43. Murdoch & Anderson, *supra* note 34, at 57-58.

44. *Id.* at 59.

45. *Id.* at 59-60. There are also other technical problems associated with TCP/IP content filtering, stemming from the fact that an entire communication may be split over several packets, making the job of filtering more complex. *Id.*

46. Zittrain & Palfrey, *supra* note 1, at 32-33.

47. Children's Internet Protection Act, 20 U.S.C. § 9134 (2010) [hereinafter CIPA].

48. *Children's Internet Protection Act,* FED. COMMC'NS COMM'N, http://www.fcc.gov/cgb/consumerfacts/cipa.html (last visited April 1, 2011).

ensure filtering takes place through the imposition of liability on ISPs.[49] Registration requirements facilitate government's gathering information about those using the Internet, including IP addresses visited and the location from which the Internet was accessed. Finally, governments often take steps to encourage self-monitoring by Internet users. Encouraging self-monitoring most often happens as a result of publishing information regarding online surveillance programs.[50]

C. Physical Location of Filtering

The choice of where to filter is no longer an easy decision, as most states do not fully control access to the Internet or directly control the ISPs that provide access to the Internet.[51] Thus, these states may be forced to rely on private or semi-private ISPs to conduct blocking on the State's behalf.[52] Common loci of Internet filtering include the source of the offending content, the ISP responsible for supplying the offending content, the destination or user's computer, and the destination ISP.[53]

Targeting the source of the offending content can be particularly effective as the source is "almost always most clearly and directly legally responsible for" distribution.[54] However, targeting the source creates two problems. First, the individual or corporation that owns the source of the offending content may be difficult to determine.[55] Second, if the source is not located within the geographic territory of the filtering state it can be difficult to change their behavior. Another related option is to target the ISP for the source of the offending content. From the perspective of enforcement this option may be more effective because "it may be easier to find and engage an ISP regarding its legal responsibilities than a single subscriber of that ISP."[56] However, this means of filtering the offending content does not resolve the second problem, because the ISP may be located abroad.[57]

---

49. *See* Communications Decency Act of 1996, 47 U.S.C. § 230 (c) (2010) (providing immunity for interactive computer service providers who are not information content providers of offensive material).

50. Zittrain & Palfrey, *supra* note 1, at 33.

51. *Id.*

52. *Id*.

53. Zittrain, *supra* note 36, at 659-73.

54. *Id.* at 659.

55. *Id.* at 662.

56. *Id.* at 669.

57. *See e.g.*, David Post, *The Iceland of the Internet*, The Volokh Conspiracy (Jan. 8, 2010), http://volokh.com/2010/01/08/the-iceland-of-the-internet (commenting that a small movement of people are interested in establishing Iceland as "a jurisdictional 'safe haven' for information on the global network" with "a set of highly-protective laws for anonymity protection, free expression, immunities for information providers, and the like for those who make information available on the net.").

Second, a government could try to target the destination or the destination ISP. Filtering at the destination has the potential to be very effective, as seen through the FCC's implementation of CIPA. In the U.S., however, even these modest efforts have met significant First Amendment challenges "grounded largely in filtering software's inaccurate categorization and therefore overbroad blocking of Web sites."[58] Consequently, filtering at the destination remains problematic unless there are sympathetic or controlled third-party owners of the computers, as in the library and school setting.[59] Filtering at the destination might become significantly more appealing and feasible if the devices used to connect to the Internet become increasingly subject to the control of third-parties, as in the case of cell phones and telecommunications companies, who have a vested interest in staying in the FCC's good graces, even at the expense of consumer preferences.[60]

Filtering at the destination ISP is perhaps the most fruitful of all the four points of control, despite not being widely used in the U.S. Destination ISPs are by their very nature local. Furthermore, the proper incentives for ISPs to conform their behavior to the legal regime of the destination country are already in place.[61] Finally, destination ISPs would be comparatively easy to control because a relatively small number of ISPs provide the vast majority of Internet users with access to the Internet.[62] Because of these advantages, controlling the destination ISPs "has been the approach of governments that wish to control the flow of content over the Internet but who cannot project that control beyond their boundaries."[63]

D. Actors Involved in Internet Filtering

Contrary to popular understanding, and wishes from the 1990s, the Internet has not eliminated the need for intermediaries. There is not now and nor is there ever likely to be a global community where individuals interact directly without the need for intermediaries.[64] Instead, the world has witnessed a transformation of the identity of the intermediaries and they have grown in number and importance. Today,

58. Zittrain, *supra* note 36, at 670.

59. *Id.* at 671.

60. *Id*. Zittrain points to the example of digital rights management initiatives seeking to design computers "that inherently manage content according to publishers', rather than users, wishes." *Id.* One could imagine a world in which cell phone carriers or manufactures moved in this direction. *Id.*

61. *Id.* at 673.

62. *Id*.

63. *Id*.

64. Goldsmith & Wu, *supra* note 27, at 71 (noting that local intermediaries "are a defining, and therefore ineliminable, aspect of the Internet.").

the Internet relies on ISPs, search engines, browsers, manufacturers of physical network components such as servers and routers, and financial intermediaries to function.[65] Notably, the vast majority, if not all, of these intermediaries are private actors.

These intermediaries have become both capable of filtering the Internet and the targets of Internet filtering pressure. Intermediaries, such as destination ISPs, discussed above, are a good target for government pressure because they too are local by definition. The presence of local intermediaries allow governments to "affect[ ] Internet flows within their borders even though they originate abroad and cannot easily be stopped at the border."[66]

The most prominent and likely future filterers of the Internet are ISPs and software companies. First, ISPs are likely to be a key player because of the potential power they can wield when filtering the Internet as nations like Saudi Arabia and China have shown. Furthermore, as previously noted, destination ISPs are local and thus easily controlled through traditional methods of government regulation. However, recent events have shown limitations exist regarding the amount of pressure nations can place on intermediaries to filter content. In late March 2010, Google decided to leave China completely and relocate to Hong Kong after Google was reportedly hacked by individuals who were trying to spy on Chinese dissidents.[67] Traffic from the Google China site, google.cn, was redirected to the Google Hong Kong site, google.com.hk, and Google will no longer censor the search results it generates.[68] In a similar move, GoDaddy.com, the largest domain service, announced it would not register new domain names in China.[69] Despite these powerful statements by Google and GoDaddy.com, other U.S. companies with a strong Internet presence, such as Microsoft and Yahoo!, have not left the Chinese market.[70]

Second, a growing trend among states that conduct state-mandated Internet filtering is to employ the services of commercial software companies who help develop and implement block lists.[71] These services work by generating lists of IP addresses or URLs, using proprietary

65. *Id.* at 70.

66. *Id.* at 68.

67. *Google Taking a Lonely Stand Against China,* CHICAGO DAILY HERALD, Mar.31, 2010, at 12.

68. Editorial, *Google and China*, N.Y. TIMES, Mar. 23, 2010, http://www.nytimes.com/2010/03/24/opinion/24wed2.html?ref=todayspaper.

69. Tony Romm, *World's Top Domain Name Service to Stop Offering Web Addresses in China,* THE HILL, (Mar. 24, 2010, 12:45 PM), http://thehill.com/blogs/hillicon-valley/technology/88843-worlds-top-domain-name-service-to-stop-offering-web-addresses-in-china.

70. *Google Taking a Lonely Stand Against China, supra* note 67.

71. Zittrain & Palfrey, *supra* note 33, at 38. (noting that U.S.-based Secure Computing's SmartFilter, Websense and Fortinet appear to assist in Internet filtering abroad).

methods, related to topics such as pornography or drugs, that will be blocked if the state uses their services.[72] These lists can also be tailored by the state purchasing the service. Thus, if a state purchases a block list related to religion, the state can tailor the list to reflect its particular ideological preferences.[73]

Beyond the manufacture of filtering programs, software companies create the programs that allow Zittrain's "appliancized" devices to access the Internet. Software companies possess the power to reprogram these devices without the consent of their users. Consequently, the software companies will have the capacity to control the manner in which users experience the Internet, including the content they are able to access.

E. Problems Associated with Internet Filtering

Internet filtering conducted by the use of IP and URL block lists is usually simultaneously overbroad and under inclusive. At the very least, it suffers from one of these two problems.[74] This lack of precision usually flows from a simple lack of resources. Although some commentators argue that "Internet filtering is almost impossible to accomplish with any degree of precision,"[75] the real roadblock is not lack of technological means but rather lack of *affordable* technology. Countries face a choice between using internally developed filtering software or purchasing software from commercial manufacturers. Due to the sheer size of the Internet and the difficulty associated with creating and updating block lists,[76] many states purchase blocking software.

The blocking lists, whether based on URLs or IP addresses, themselves are imperfect methods. Blocking based on IP addresses is particularly susceptible to the criticism that it is overbroad because it blocks everything at a given IP address rather than distinguishing between permissible and impermissible content.[77] For example, Spain blocked the entire IP address associated with the terra.es domain, when only one page hosted on that domain had offending content.[78] Furthermore, IP addresses are not entirely static. From time to time, IP addresses are reassigned and, unless the blocking list is updated, innocuous content may be blocked.[79] Blocking based on URL address faces much the same

72. *Id.*
73. *Id.* at 38-39.
74. *Id.* at 46.
75. *Id.*
76. *Id.* at 38. (noting that the task of Internet filtering is further complicated when sites realize they are the target of blocking attempts and attempt to thwart the blocking by changing their URL addresses).
77. *Id.* at 46.
78. Zittrain, *supra* note 36, at 653.
79. *Id.*

problem. Notably, URL blocking is even more resource intensive than IP address blocking and thus it is used primarily in Saudi Arabia and China.[80] One problem likely to grow in importance is the blocking of blogs. Individual blogs hosted by a service all have similar URL addresses so countries are forced to either block blogs individually, which is resource-intensive, or to block the entire blog service at the URL level, *i.e.* blocking all of http://freespace.virgin.net as Saudi Arabia was doing, as of 2004.[81]

The lack of affordable technological means to conduct Internet filtering also causes under inclusive Internet filtering. As noted previously, the manufacturers of blocking list technology are American companies. Thus, their programs tend to target more English language websites rather than websites in the local language, where the latter generally cause more concern for states electing to filter the Internet.[82] This potentially results in under inclusive blocking where impermissible content available in English is blocked but the same content written in the local language is freely accessible.[83] Furthermore, Internet filtering need not be "be completely effective to be adequately effective."[84] Goldsmith and Wu explain, and Zittrain seemingly would agree, filtering efforts need only make it sufficiently difficult that the majority of users will not attempt to access a given website.[85] Nonetheless, OpenNet Initiative has found that the overall trend is towards an increase in Internet filtering and an increase in the number of methods employed to achieve Internet filtering goals.[86]

III. WTO COMMITMENTS GOVERNING INTERNET FILTERING

The GATS Agreement, specifically Articles XIV and XVI, in combination with an individual country's Schedule of market access commitments, provides the basic legal text governing commitments applicable to the Internet and e-commerce. When the WTO Agreements were drafted there was no Internet as we know it today. Thus none of the WTOs legal instruments, including the GATS Agreement were drafted with the Internet in mind. As a result, it is quite challenging to stretch these agreements to cover the Internet, while ensuring they are inter-

80. *Id.*

81. Zittrain & Palfrey, *supra* note 33, at 47.

82. *Id.* at 38-39. (citing as an example the UAE decision to block English-language dating sites but no Arabic-language dating sites).

83. *Id.* at 39.

84. GOLDSMITH & WU, *supra* note 27, at 67.

85. *Id.*

86. *Id.* at 41-43 (noting "an increase in alternative modes of filtering, both in engineering techniques and through increased licensing, registration, and reporting requirements in some states.").

preted in a consistent and meaningful fashion. The *U.S.-Gambling Services* case was the first, and remains the only case, to attempt to apply the GATS Agreement rules in the context of an Internet service. As a result, predicting how the GATS Agreement will be interpreted to apply to Internet filtering cases is challenging. Such interpretation raises questions of whether products delivered via the Internet should be classified as goods or services. If classified as services, what Mode (method of supplying the service) the service falls within must also be determined as it has the potential to affect the national law governing the transaction. While the *U.S.-Gambling Services* decision clarified many of these points, areas of uncertainty remain.

A. GATS Agreement

The GATS Agreement, covering trade in services, is one of the treaties comprising the WTO's legal framework. The GATS Agreement sets specific rules regarding market access barriers, which are typically tariffs and non-tariff barriers that impede entry into a given market, and their gradual reduction. These rules do not prohibit market access barriers, but rather prohibit a WTO Member from affording other Members treatment *less favorable* "than that provided for under the terms, limitations and conditions agreed and specified in its Schedule."[87] Thus, Member countries agree to certain market access commitments, in a bottom-up rather than top-down fashion, and those commitments are memorialized in the country's Schedule.

GATS commitments are made in specific sectors and based on a specific mode of delivery. WTO members can make commitments in twelve broad sectors: business services, communication services, construction and related engineering services, distribution services, educational services, environmental services, financial services, health-related and social services, tourism and travel-related services, recreational, cultural and sporting services, transport services, and other services.[88] Each sector is divided into subsectors. The sectors that are most important to a discussion of e-commerce or electronically supplied services are (listed as broad service – subsector): business services - computer and related services; communication services - value-added telecommunications services; recreational, cultural and sporting services - entertainment services (section under which gambling services were held to fall in *U.S.-Gambling Services* decision);[89] and communication services - audiovisual

87. General Agreement on Trade in Services art. XVI, para 1, art. XIV(a), Apr. 15, 1994, 1869 U.N.T.S. 183.

88. Peter Van den Bossche, The Law and Policy of the World Trade Organization: Text, Cases and Materials 485 (2d ed. 2008).

89. U.S. – Gambling Services Appellate Body Report, paras.162 – 168.

services.[90]

Second, commitments are made in one of four modes. The four modes of supply are: cross-border supply (Mode 1); consumption abroad (Mode 2); supply through commercial presence (Mode 3); and supply through presence of national persons (Mode 4).[91] Under the GATS Agreement nations are permitted to make different commitments in each of the modes of supply.

B. Exceptions to the GATS Agreement

The GATS Agreement permits countries to deviate from their Schedule of market access commitments to protect (1) public morals and order, (2) human or animal welfare, (3) or to ensure compliance with domestic laws not inconsistent with the GATS Agreement. Specifically, Article XIV of the GATS Agreement provides:

> Subject to the requirement that such measures are not 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 services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> a. necessary to protect public morals or to maintain public order;
> b. necessary to protect human, animal or plant life or health;
> c. necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those related to:
> i. the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
> ii. the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
> iii. safety;
> d. inconsistent with Article XVII, provided that the difference in treatment is aimed at ensuring equitable or effective imposition of direct taxes in respect of services or service suppliers of other Members;
> e. inconsistent with Article II, provided that the difference in treatment is the result of an agreement on the avoidance of double taxation or provisions on the avoidance of double taxation in any other international agreement or arrangement by which the Member is bound.

Article XIV has been interpreted to require satisfaction of a two-tier test to justify otherwise GATS inconsistent measures. In the *U.S.-Gam-*

90. Sacha Wunsch-Vincent, The WTO, the Internet and Trade in Digital Products: EC-US Perspectives, 68 (2006).

91. Van den Bossche, *supra* note 88, at 486-87.

bling Services decision, the Appellate Body said that it would first look to see "whether this measure can provisionally be justified under one of the specific exceptions under paragraphs (a) to (e) of Article XIV."[92] If so, the Appellate Body will see "whether the application of this measure meets the requirements of the *chapeau* of Article XIV."[93] The *chapeau*[94] of Article XIV forbids the challenged measure from being applied in a discriminatory manner, even if it is otherwise compliant with an exception specified in paragraph (a) - (e). For example, if certain filtering were needed to protect public morality, but was applied so as to block content from England but not France, that measure would not constitute a valid exception to a nation's market access commitments because it would fail to satisfy the requirements of the *chapeau*.

The exception most likely to apply to the e-commerce and electronically supplied services context, and the one encountered in the *U.S.-Gambling Services* case, is for the protection of public morals and maintenance of public order.[95] This exception, along with the exceptions in paragraphs (b) and (c) imposes a further consideration. For a measure under paragraph (a) – (c) to be provisionally justified it must be *necessary* to achieve the policy objective pursued.[96]

The necessity of an otherwise impermissible measure is in turn measured by a two-tiered test. In particular, Article XIV(a) requires that to be provisionally justified the invoking Member must show that: "the policy objective pursued by the measure at issue is the protection of public morals or the maintenance of public order; and the measure is necessary to fulfill that policy objective."[97] A full discussion of how this requirement was interpreted by the Appellate Body in *U.S. –Gambling Services* and how it might apply to future Internet filtering cases is provided in Part IV.

C. Problems Associated With Applying the WTO GATS Commitments to e-Services

At the time the GATS Agreement was drafted, between 1986 and 1994,[98] the Internet as we know it did not exist. The Internet that did

92. *Id.* at 654.

93. *Id.*

94. The *chapeau*, French for hat, refers to the first sentence of Article XIV that precedes paragraphs (a) – (e).

95. General Agreement on Trade in Services art. XIV(a), Apr. 15, 1994, 1869 U.N.T.S. 183(a).

96. Van den Bossche, *supra* note 88, at 654 (2d ed. 2008).

97. *Id.* at 655.

98. *See generally* Taunya L. McLarty, *Liberalised Telecommunications Trade in the WTO: Implications for Universal Service Policy*, 51 Fed. Comm. L.J. 1, 13-18 (1998). The 1986 Ministerial Declaration on the Uruguay Round paved the way for the trade in service

exist did not involve the extensive cross-border trade in services but rather was a collection of nascent and largely independent ISPs serving distinctive constituencies.[99] As a result, the legal structure of the GATS Agreement is not particularly suitable to govern e-commerce and electronically supplied services.[100]

The first problem stems from trying to decide whether e-commerce and electronically supplied services should fall within the General Agreement on Trade and Tariffs ("GATT"), which applies to trade in goods only, or the GATS Agreement. This initial problem is tricky because e-commerce is nothing more than content on a carrier medium that can now be downloaded on the Internet.[101] For example, a recording artist can supply music either in a brick and mortar store on a CD or can elect to use iTunes. In both cases the item being supplied is music, arguably a good. Should making that good available for download on the Internet make it a service rather than a good? Nowhere in the WTO legal regime is there a clear definition of what constitutes a good versus what constitutes a service.[102]

The best view is that e-commerce should be classified as services rather than goods. The first argument, initially advanced by the EU, is that the GATT Agreement was never designed to cover "information digitised [sic] into bits and sent across a border through a telecommunications network."[103] The EU further argued that such content has always been considered as computer or audiovisual services and thus subject to the GATS Agreement.[104]

Second, the WTO does not provide for a rule guaranteeing technological neutrality between the GATS and the GATT.[105] In other words, the same good need not be treated similarly when it is transmitted over different media. In fact, the GATS Agreement itself enshrines unequal

---

negotiations. *Id.* Negotiations concluded in 1994, after the U.S. recommendation was accepted, dividing services into six parts. *Id.*

99. For example, Compuserve, which was more business and technically focused, and Prodigy, which marketed itself as family-oriented.

100. *See* WUNSCH-VINCENT, *supra* note 91, at 71 (2006) (noting that "most of the digital content services . . . are inseparable combinations of telecommunications, software and audiovisual services that rely on commitments on these content services themselves and their digital transmission").

101. *Id.* at 48.

102. *Id.* at 49.

103. *Id.* at 56 (citing GC, Submission for the EC, Classification Issues and the Work Programme on E-Commerce, WT/GC/W/497 (9 May 2003) para. 7).

104. *Id.* at 56.

105. *Id.* at 56 (noting "the likeness of products between content being exported on physical carrier media and content delivered electronically does not imply an obligation to afford identical trade treatment.").

treatment by allowing for different commitments across the four different modes of supply.

Finally, legal certainty is increased and economy of resources promoted if a GATS Agreement rather than a GATT classification is used. The EU has argued that if electronic deliveries are classified in accordance with their "physical equivalent under the GATT, many physical outcomes (*e.g.,* blueprints) that result from services (*e.g.,* architectural, consulting services) hitherto clearly targeted by the GATS would have to be considered under the GATT," resulting in a significant re-classification of otherwise already classified services.[106] Thus, one of the advantages of using a GATS classification is avoiding the re-classification negotiations that would be required.[107]

The second problem commonly associated with the extension of GATS classifications to e-commerce and electronically delivered services is whether such services should be considered Mode 1 or Mode 2 services. The Mode classification is relevant because the extent of liberalization undertaken in each of the Modes varies. Typically, commitments made under Mode 2 are more liberal than commitments made under Mode 1.[108] However, increasingly nations are making commitments that are the same across Modes 1 and 2.[109]

The question of whether e-commerce and electronically traded services should be classified under Mode 1 or Mode 2 turns on "whether the service is produced abroad and sent across borders to a foreign consumer or whether it is the consumer who 'travels' abroad to consume a service."[110] However, in the context of e-commerce this definition is hard to apply. Consider the circumstance of the service that is produced abroad and hosted on a server abroad. That service still could be considered to be sent across a border because the service is accessible from within the territory of a foreign country. Hence, it could be classified as a Mode 1 service. Conversely, one might say that the service does not cross the border of another country because it is not hosted on a server within that country. Instead, the consumer 'travels' to the server located abroad. Under this understanding the service would more properly be classified as a Mode 2 service.

One suggested resolution of this definitional problem is to focus on whether the service provider actively approaches the consumer, which would be Mode 1, or whether the consumer approaches the provider

106. WUNSCH-VINCENT, *supra* note 91, at 59.

107. *Id.* at 60.

108. *Id.* at 67.

109. Sacha Wunsch-Vincent, *The Internet, Cross-Border Trade in Services and the GATS: Lessons from US-Gambling*, 3 WORLD TRADE REV. 319, 324 (2006).

110. WUNSCH-VINCENT, *supra* note 91, at 65 (citing Article I, para 2 of the GATS Agreement).

through a visit to a website, which would be Mode 2.[111] This solution, however, leaves much to be desired. The service provider could solicit the customer over a different media, such as television, and request that the customer visit his website. What modal classification would be appropriate under this scenario? Another solution would be to classify e-commerce as the predecessors of e-commerce, telephone and fax services, were classified. Historically, telephone and fax services were classified as Mode 1.[112]

A third problem, arising from the uncertainty surrounding the classification of e-services, is the jurisdictional questions that different modal classifications might raise. The basic question in the case of e-services is which national legal system should govern a cross-border transaction: the country of the supplier or the country of the consumer?[113] Some commentators have argued that modal classification answers this debate, while others argue that modal classification does not have a jurisdictional implication.[114] If modal classification were determinative, Mode 1 would secure the primacy of the consumer's locality because the business transaction would be deemed to have occurred in the consumer's locality.[115] Conversely, Mode 2 would implicate the legal system of the supplier's locality as the prevailing law.[116]

D. The WTO U.S.-Gambling Services Decision

The *U.S.-Gambling Services* decision remains the only WTO decision regarding the provision of Internet services and the only decision directly applicable to a discussion of how the WTO legal regime could be applied to Internet filtering. It is a landmark decision because it confirms two basic facts that are crucial to a complete discussion of how GATS commitments would apply to future Internet filtering cases. First, the *U.S.-Gambling Services* decision confirms that WTO GATS commitments are applicable to e-commerce and electronically supplied services.[117] Second, the *U.S.-Gambling Services* decision clarified that e-commerce and electronically supplied services will be treated under Mode 1, and not Mode 2.[118]

111. *Id.* at 66.

112. *Id*. at 67.

113. *Id*. at 68. Although historically there has been some question regarding whether it was even possible to identify the country of the supplier, the increased availability and affordability of geolocation technologies has largely quashed this concern.

114. *Id.*

115. *Id.*

116. *Id.*

117. Wunsch-Vincent, *supra* note 109, at 3.

118. Wunsch-Vincent, *supra* note 90, at 175.

The first part of the decision was largely expected and the decision did nothing more than confirm the general understanding of academics: that e-commerce and electronically delivered services are governed by the GATS Agreement. Given the time that has passed since the decision and the general academic consensus on this issue, it seems unlikely that the WTO would retreat from the decision.

However, the second clarification, regarding the decision to treat e-commerce and electronically supplied services as Mode 1, was not as expected. Nonetheless, the WTO Appellate Body, in concluding that e-commerce and e-services are governed by Mode 1, has done nothing more than national courts have in terms of trying to solve this thorny question.

If one believes that modal classification has jurisdictional effects, then a Mode 1 classification would mean that the law of the consumer's locality should prevail in debates over the appropriateness of Internet content. Domestic courts have previously reached just this conclusion. In April of 2000, La Ligue Contre Le Racisme et L'Antisemitisme ("LICRA"), filed suit in French court against Yahoo objecting to Yahoo's presentation of Nazi memorabilia for sale on its websites, in violation of French law.[119] The French court issued an order on May 22 that in essence required Yahoo to stop this content from being viewable by users from within France.[120] The significance of this order is that it shows that French courts, as early as mid-2000, believed they had the right to control Internet content being projected into their country, just as the WTO reaffirmed with its classification of e-services as Mode 1 rather than Mode 2.

Other European courts have similarly held that foreign owned and operated websites are required to follow national laws, if their websites are viewable inside that country. For example, in 2000, the Bundesgerichthof, Germany's highest court, held that an Australian website was required to follow German anti-Nazi speech and Holocaust laws.[121] An Australian national had posted Holocaust revisionist material on his website and the Bundesgerichthof ordered its removal.[122] Italian courts have also held that Italian libel laws apply to all online content viewable in Italy.[123]

---

119. Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d 1199, 1201-1203 (9th Cir. 2006).

120. *Id*. at 1202-03.

121. Mahasti Razavi & Thaima Samman, *Yahoo! and Limitations of the Global Village,* 19 COMM. LAW. 27, 28 (2001).

122. Julie L. Henn, Note, *Targeting Transnational Internet Content Regulation*, 21 B.U. INT'L L.J. 157, 171 (2003).

123. Razavi & Samman, *supra* note 121, at 28.

IV. U.S. INTERNET FILTERING EFFORTS AND WHY THEY ARE UNLIKELY TO VIOLATE WTO GATS COMMITMENTS

The U.S. government is not engaged in extensive Internet filtering, but rather has chosen to concentrate its filtering efforts in areas that fall well within the accepted GATS Agreement morality and public order exceptions. The prime and perhaps only example of U.S. governmental filtering is conducted pursuant to CIPA through the FCC's implementation of the E-rate program.[124] Similarly, the amount of filtering conducted by private entities is limited. However, unlike governmental filtering that is restricted by U.S. First Amendment doctrine, filtering conducted by private entities has great potential to increase. Nonetheless, U.S. filtering efforts are unlikely to prompt a future WTO case, as the *U.S.-Gambling Services* Case was unique and is unlikely to be repeated.

A. Internet Filtering Techniques Employed by the U.S.

Historically, the United States has opposed the regulation of the Internet and thus has not engaged in an extensive range of filtering activities. The U.S. government, in stark opposition to the approach of European nations and the European Union, feared that Internet regulation would have a negative impact on the development of e-commerce, ultimately harming the U.S. economy rather than benefitting it.[125] As a result, the majority of U.S. Internet filtering efforts have taken the form of content regulations to address the problems associated with the distribution of child pornography and more general concerns about child protection, morality, national security, intellectual property, and computer security.[126]

The U.S. has tended to rely more heavily on requesting the content supplier to remove content rather than blocking users' access to given objectionable content.[127] Moreover, U.S. Internet filtering efforts have increasingly targeted the Internet's crucial intermediaries to accomplish their filtering, as evidenced by U.S. targeting of financial intermediaries to limit access to foreign online gambling websites.[128] This paper highlights four main efforts at Internet filtering that the U.S. has conducted

---

124. *See supra* Section IIB.

125. Goldsmith & Wu, *supra* note 27, at 40-42.

126. John G. Palfrey, *Internet Filtering in the United States and Canada*, *in* Access Denied: The Practice and Policy of Global Internet Filtering 226, 226 (Ronald Diebert et al. eds., 2008).

127. Goldsmith & Wu, *supra* note 27, at 40-42.

128. Tom Newnham, *WTO Case Study: United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, 7 Asper. Rev. Int'l Bus. & Trade L. 77, 89 (2007) (citing Internet Gambling Prohibition and Enforcement Act, H.R. 4411, 109th Cong. (2005). Although H.R. 4411 never passed, substantially similar provisions targeting financial intermediaries were included in The Security and Accountability For Every Port

in recent years, as efforts illustrative of the activities that are ongoing in the United States.

The clearest example of U.S. Internet filtering conducted by the government is the forced installation of filtering software on computers in public areas accessible to children in public libraries and public schools, as required under the Children's Internet Protection Act of 2000 ("CIPA"). Under CIPA, schools and libraries who want to receive discounts for computer equipment offered by the E-rate program[129] must agree to include filtering software on their computers that "block[s] or filter[s] Internet access to pictures that are: (a) obscene, (b) child pornography, or (c) harmful to minors (for computers that are accessed by minors)."[130] Hence, although this type of filtering is included as a licensing requirement, it functions as direct content filtering for the user and is subject to the same problems of over-breadth and under-breadth as all Internet content filtering practices.

CIPA was challenged shortly after it was enacted. In 2001, the American Library Association ("ALA") in conjunction with the ACLU successfully challenged CIPA before the Eastern District of Pennsylvania,[131] but ultimately lost in 2003 before the Supreme Court.[132] At least one of the Justices, Justice Kennedy, believed that the key rationale for the Supreme Court's decision to reverse the district court and uphold the constitutionality of CIPA was the apparent ease with which the filtering could be removed to facilitate use of the Internet by adults for legitimate research purposes.[133] This reveals how the U.S. approach toward Internet filtering is tempered by concerns for First Amendment rights that are less pronounced or non-existent in other nations that engage in more comprehensive filtering efforts, such as the European Union member countries and China respectively.

Pennsylvania, like the federal government, has taken a stab at Internet filtering in much the same category of content. In February 2002,

---

Act of 2006. *See* The Security and Accountability For Every Port Act of 2006, 31 U.S.C. §§ 5361–5367 (2010).

129. *E-rate,* FED. COMMC'NS COMM'N, http://www.fcc.gov/learnnet/ (last visited Feb. 2, 2011). The E-rate program was passed as part of the Telecommunications Act of 1996. *Id.* The program facilitates library and school access to affordable telecommunication equipment and more importantly Internet access. *Id.* The program is managed by the Universal Service Administrative Company at the direction of the FCC. *Id.*

130. *Children's Internet Protection Act,* FED. COMMC'NS COMM'N, http://www.fcc.gov/cgb/consumerfacts/cipa.html (last visited Feb. 2, 2011). Under the law, adult patrons using computers with filtering technology installed my request the deactivation of the filtering technology. *Id.* Furthermore, the law does not include any Internet use tracking requirements. *Id.*

131. Am. Library Ass'n, Inc., v. United States, 201 F. Supp. 2d 401 (E.D. Pa. 2002).

132. United States v. Am. Library Ass'n Inc., 539 U.S. 194 (2003).

133. *Id*. at 214-15 (Kennedy, J., concurring).

Pennsylvania passed a law providing for censorship at the destination ISP[134] of illegal child pornography.[135] The law requires:

> An Internet service provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet service provider is notified by the Attorney General pursuant to subsection (g) that child pornography items reside on or are accessible through its service.[136]

Initially, the law prompted some objections from ISPs on the basis that they were unable to discriminate between Pennsylvania and non-Pennsylvania users of their service and thus were forced to block noticed content for all of their subscribers.[137] Again, the Pennsylvania law demonstrates how content based filtering is often subject to problems of over-breadth. In this case the over-breadth stemmed from a lack of geographic specificity.

In 2003, Zittrain noted how one federal district court had already struck down similar New York legislation on the basis that "the unique nature of cyberspace necessitates uniform national treatment."[138] Indeed in 2004, the Eastern District of Pennsylvania considered Pennsylvania's foray into Internet filtering and similarly declared the Pennsylvania law unconstitutional.[139] This ruling, however, may no longer completely foreclose similar filtering efforts as the availability and affordability of geolocation technology has increased dramatically since 2004. To the extent that the district court found the law troublesome because the law had "the practical effect of exporting Pennsylvania's domestic policies,"[140] geolocation technology may cure that problem. Nonetheless, advances in geolocation technologies will not remedy concerns based on First Amendment arguments and the tendency of content-based regulations to block access to innocent as well as the target websites.

The U.S. military also conducts Internet filtering. In August 2009, the U.S. Marine Corps banned social networking sites.[141] Based on limited information in the press, it seems that the ban will be enforced at

134. Jonathan Zittrain, *Internet Points of Control,* 44 B.C L. REV. 653, 674 (2003) (noting China conducts much of its filtering via content filtering at the destination ISP).

135. *Id*.

136. 18 PA. CONS. STAT. § 7330(a) (2002).

137. Zittrain, *supra* note 37 at 675-76.

138. *Id*. at 676 (quoting Am. Library Ass'n v. Pataki, 969 F. Supp. 160, 184 (S.D.N.Y. 1997)).

139. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004).

140. *Id*. at 662.

141. *2009 Year in Review*, OPENNET INITIATIVE, http://opennet.net/about-filtering/2009 yearinreview/# (last visited Feb. 2, 2011).

the destination ISP.[142] The articulated rationale was security concerns both on the operation side and in terms of computer security.[143] Interestingly, the military has a far from uniform stance on social networking sites and Web 2.0 applications, with the Army ordering all U.S. bases to provide access to Facebook and the Defense Department considering a department-wide ban on Web 2.0 sites.[144]

The most well-known instance of Internet filtering by the U.S. has been government attempts to prevent U.S. residents from participating in Internet gambling. This type of filtering was somewhat unique because it was accomplished not by blocking the Internet gambling websites themselves, but rather by targeting the financial intermediaries, specifically credit card companies and banks that served the online gambling websites. Both Congress and individual states enacted laws to prevent financial intermediaries from doing business with the online gambling companies.[145] Targeting Internet intermediaries, through which many Internet activities must pass, is likely to prove an increasingly fruitful means of accomplishing Internet filtering.

Other sporadic blocking appears to be taking place as well, although finding out about it is somewhat luck of the draw. In late July, OpenNet Initiative learned that AT&T had very briefly blocked access to 4chan.org for customers in Southern California.[146] The ban allegedly only lasted several hours and was reported on several social media sites, such as Twitter and Reddit.[147] At least one news source confirmed with

142. Noah Shachtman, *Marines Ban Facebook, Twitter, Other Sites*, CNN.COM (Aug. 4, 2009), http://edition.cnn.com/2009/TECH/08/04/marines.social.media.ban/index.html (noting that the ban will block the sites from U.S. Marine networks).

143. *Id.* at 143.

144. *Id.*

145. *See e.g.,* Kiran S. Raj, Comment, *Drawing a Line in the Sand: How the Federal Government Can Work with the States to Regulate Internet Gambling*, 56 EMORY L.J. 777, 789 (2006) (noting that the Unlawful Internet Gambling Enforcement Act, 31 U.S.C. § 5361 et seq. (2006), made "it illegal for a bank to process, and for any Internet gambling operator to receive, funds in connection with gambling activities considered illegal under other federal or state laws"); Kevin F. King, *Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot,* 11 COLUM. SCI. & TECH. L. REV. 41, 46 (2010) (noting that enforcement of federal Internet gaming laws are "enforced via Department of Justice investigations and Treasury Department regulations requiring banks to block transfers to Internet gambling providers"); Prohibition on Funding of Unlawful Internet Gambling, 73 Fed. Reg. 69, 382 (Nov. 18, 2008) (to be codified at 12 C.F.R. pt. 233; 31 C.F.R. pt. 132); Joel D. Reidenberg, *Current Debates in the Conflict of Laws: Choice of Law and Jurisdiction on the Internet: Technology and Internet Jurisdiction*, 153 U. PA. L. REV. 1951, 1960 (2005) (explaining New York's successful campaign to stop banks from processing transfers to Internet gaming sites).

146. *2009 Year in Review*, *supra* note 141.

147. Ben Parr*, Report, AT&T Blocking 4chan*, MASHABLE (July 26, 2009), http://mashable.com/2009/07/26/report-att-blocking-4chan/.

AT&T that they were intentionally blocking the website.[148] One plausible explanation for AT&T's blocking of 4chan.org, stems from its notoriety for Internet pranks and hacking efforts.[149] One report confirms this explanation:

> Beginning Friday, an AT&T customer was impacted by a denial-of-service attack stemming from IP addresses connected to img.4chan.org. To prevent this attack from disrupting service for the impacted AT&T customer, and to prevent the attack from spreading to impact our other customers, AT&T temporarily blocked access to the IP addresses in question for our customers. This action was in no way related to the content at img.4chan.org; our focus was on protecting our customers from malicious traffic. Overnight Sunday, after we determined the denial-of-service threat no longer existed, AT&T removed the block on the IP addresses in question. We will continue to monitor for denial-of-service activity and any malicious traffic to protect our customers.[150]

At this point, blocking by individual ISPs does not appear to be especially common. It is hard to speculate whether its use is likely to increase. Although United States First Amendment principles would not govern filtering actions by private ISPs, unless conducted pursuant to government direction, it seems unlikely that ISPs would resort to such measures because the First Amendment is deeply ingrained in U.S. culture.

B. U.S. Filtering Efforts are Unlikely to Violate GATS Commitments

1. *Nature of U.S. WTO GATS Commitments*

The U.S. has made GATS commitments across most of the services sectors. In the area of telecommunications services, which includes many Internet based services and content, the U.S. imposes no significant market access restrictions for Mode 1 supply of telecommunications services.[151] Similarly, in the area of audiovisual services, the U.S. has not imposed any significant market access restrictions.[152] These categories would likely cover all future Internet filtering actions, with the exception of any future actions regarding online gambling, which would again be classified under Recreational, Cultural, and Sporting Services.

148. David Murphy, *AT&T Blocks 4chan, Stirs Internet Hornet's Nest*, PCWorld (July 27, 2009), http://www.pcworld.com/article/169079/atandt_blocks_4chan_stirs_Internet_hornets_nest.html (reporting that Centralgadget.com confirmed AT&T was "currently blocking portions of the Internet site 4chan.org.").

149. Parr, *supra* note 147.

150. Murphy, *supra* note 149.

151. United States' Schedule of Specific Commitments under the General Agreement on Trade in Services, S/DCS/W/USA (Feb. 27, 2003).

152. *Id.*

However, the U.S. has revoked its commitments regarding sporting services.[153]

2. *Exceptions to GATS Commitments*

The GATS Agreement allows countries to derogate from their market access commitments provided they satisfy certain guidelines set forth under Article XIV. In *U.S. – Gambling Services*, the Appellate Body interpreted the meaning of the exceptions found in Article XIV and applied them in the gambling context. Specifically, Antigua had challenged the use of the Wire Act, the Travel Act, and the Illegal Gambling Business Act to prohibit online gambling providers located abroad from providing their services within the United States. To test whether the U.S. restrictions on Antiguan suppliers of gambling services were legal the Appellate Body first looked to see whether the challenged measure fell within the scope of paragraphs (a) – (e) of Article XIV which "requires the challenged measure to address the particular interest specified in that paragraph and that there be a sufficient nexus between the measure and the interest protected."[154] If the challenged measure provisionally satisfied that test, the Appellate Body examined whether the measure complied with the *chapeau*'s requirement that the measure be applied in a non-discriminatory manner to similarly situated countries.[155]

With regard to the protection of public morals and the maintenance of public order the Appellate Body held that the challenged measure must be *necessary* to achieve the desired policy objective.[156] To assess whether a challenged measure is necessary the Appellate Body again created a two-tiered test requiring the invoking Member to show that "the policy objective pursued by the measure at issue is the protection of public morals or the maintenance of public order; and the measure is necessary to fulfil [sic] that policy objective."[157]

The Panel decision dealt extensively with the meaning of public morals and public order and was upheld but not discussed extensively by the Appellate Body.[158] The Panel concluded that Members had "some scope to define and apply for themselves the concepts of 'public morals' and 'public order' in their respective territories, according to their own

153. *Q&A on Impact of U.S. Compensation Offer in GATS Article XXI: Negotiations regarding Gambling Services on U.S. Laws and Regulations*, OFFICE OF THE U.S. TRADE REPRESENTATIVE, http://www.ustraderep.gov/assets/Trade_Sectors/Services/asset_upload_file515_15526.pdf.

154. U.S. – Gambling Services Panel Report, *supra* note 5.

155. *Id*.

156. *Id*.

157. VAN DEN BOSSCHE, *supra* note 88.

158. U.S. – Gambling Services Panel Report, *supra* note 5.

systems and scales of values."[159] Furthermore, the Panel accepted the argument by the U.S. that Internet gambling posed risks to public morals and public order in the form of organized crime, money laundering and fraud, risks to children, and risks to health from gambling addiction.[160]

The Panel and the Appellate Body disagreed over the necessity element of the challenged measures. The Panel found that the U.S. had not sufficiently demonstrated that the challenged measures were necessary,[161] but the Appellate Body reversed that finding and instead held that the challenged measures were necessary.[162] The Appellate Body's holding rested on whether there were alternative measures "reasonably available" that the U.S. had not pursued. Significantly, the Appellate Body commented that "[a]n alternative measure may not be 'reasonably available,' however, where it is merely theoretical in nature, for instance, where the responding Member is not capable of taking it, of where the measure imposes an undue burden on that Member, such as prohibitive costs or substantial technical difficulties." They went on to find that Antigua's offer of consultations was not a measure 'reasonably available' to the U.S. and thus that the three federal statutes satisfied the necessity standard under Article XIV.[163]

However, the Appellate Body then went on to evaluate whether the measures were consistent with the *chapeau* of Article XIV, which requires that the challenged measure be applied in a non-discriminatory manner as to similarly situated countries. The Appellate Body upheld the Panel's findings that the provisions of the International Horseracing Act discriminated between foreign and domestic service suppliers and thus violated the *chapeau* of Article XIV.[164] Specifically, the Appellate Body noted that the International Horseracing Act authorized domestic service suppliers, but not foreign service suppliers, to offer remote better services and it was this differentiation in treatment in countries where like conditions prevailed that violated the *chapeau* of Article XIV.[165]

---

159. *Id*.

160. *Id*.

161. *Id*.

162. *Id*.

163. *Id*.

164. U.S. – Gambling Services Panel Report, *supra* note 5. Additionally, after U.S. compliance with the Appellate Body's decision was not forthcoming, Antigua requested the establishment of an Article 21.5 Panel. The Panel clarified the scope of the Appellate Body's decision stating that "the U.S. was *not entitled* to maintain its offending measures – the *Wire Act*, the *Travel Act*, and the *Illegal Gambling Business Act* – under the 'public morals' exception." Newnham, *supra* note 128, at 93-94.

165. U.S. – Gambling Services Panel Report, *supra* note 5.

3. *Current Filtering Efforts Do Not Violate U.S. GATS Commitments*

Current U.S. filtering efforts, particularly those accomplished through the FCC's implementation of CIPA, are extremely unlikely to be found in violation of U.S. commitments under the GATS Agreement. The specific policy objectives pursued by CIPA are objectives explicitly designed to protect the health and safety of children. Protecting the health and safety of children categorically falls within the Panel's definition of a public moral, which states public morals are "standards of right and wrong conduct maintained by or on behalf of a community or nation."[166] Additionally, preventing the dissemination of obscene material, particularly child pornography, would also certainly fall within the Panel's articulation of the public order. Public order, according to the Panel, means "the preservation of the fundamental interests of a society, as reflected in public policy and law. These fundamental interests can relate, *inter alia*, to standards of law, security and morality."[167] Furthermore, even though this would not be required under WTO GATS jurisprudence, practically speaking much of the underpinning for CIPA stems from moral policy objectives that are accepted almost universally, such as preventing children from being exposed to obscene or pornographic material, and as such would be unlikely to draw objection from other countries.

A second reason that U.S. filtering efforts are unlikely to violate GATS commitments lies in the fact that U.S. commitments to the WTO under the GATS Agreement are significantly less stringent than the level of review imposed by U.S. courts under First Amendment principles. Practices that could potentially violate WTO Commitments would almost always be found in violation of the First Amendment and halted before a WTO challenge was mounted. First Amendment principles operate as an important restriction on the scope of U.S. Internet filtering both in terms of legal limitations and social limitations. As a result of U.S. First Amendment jurisprudence, more extreme types of Internet filtering have not taken place in the U.S. and nor are they likely to develop in the future.[168] For example, states, such as Pennsylvania, have tried to regulate Internet content within their state have had their regulations struck down as unconstitutional on First Amendment grounds. Finally, the CIPA filtering blocks all websites equally and does not discriminate based on the source of the content, unlike the challenged U.S. gambling regulations.[169]

166. *Id*.

167. *Id*.

168. GOLDSMITH & WU, *supra* note 27, at 40-42; Palfrey, *supra* note 233.

169. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 666. (E.D. Pa. 2004).

Recently, at least one prominent U.S. company, Google, has come out publicly and strongly against Internet filtering. On March 24, 2010, Google executive, Alan Davidson, speaking before the Congressional Executive on China, commented on the threat Internet filtering posed to international trade.[170] Google supported its rhetoric against filtering by leaving the Chinese market and closing its previously censored search site Google.cn as of March 22, 2010.[171] With such prominent companies, especially ones that are well positioned to carry out Internet filtering, coming out against Internet censorship, it seems unlikely that the U.S. would suddenly decide to increase its own filtering efforts, as other nations like Australia have recently chosen to do.[172]

4. *The U.S.-Gambling Services* Case Was Unique and is Unlikely to be Repeated

The *U.S.–Gambling Services* case was unique in two important respects: (1) it concerned the importation of a service, Internet gambling, when the U.S. is predominantly an exporter of services rather than an importer, and (2) the *U.S.-Gambling Services* decision resulted from a complete denial of market access in a given sector, whereas the limited filtering conducted by the U.S. outside of that conducted under the FCC's implementation of CIPA does not cause a complete denial of market access.

First, the U.S. is predominantly an exporter of services.[173] Although the U.S. does import a considerable amount of services "the United States continues to maintain the largest services trade surplus of any country in the world" demonstrating that its services exports far exceed its imports as compared to other countries.[174] Specifically, in 2007, service exports reached $480 billion while imports totaled $341.1 billion, creating the largest services trade surplus in U.S. history and that the world has seen.[175]

Although the U.S. has yet to collect data specifically addressing the trade in e-services there is no reason to believe this correlation is any

170. Javier C. Hernandez, *Google Official Calls for Action on Web Limits*, N.Y. TIMES, Mar. 24, 2010, http://www.nytimes.com/2010/03/25/technology/25google.html?hpw.

171. Miguel Helft & David Baroza, *Google Shuts China Site in Dispute Over Censorship*, N.Y. TIMES, Mar. 22, 2010, http://www.nytimes.com/2010/03/23/technology/23google.html.

172. *Green Light for Internet Filter Plans*, ABC NEWS, (Dec. 15, 2009), http://www.abc.net.au/news/stories/2009/12/15/2772467.htm (announcing that Australia will introduce compulsory Internet filtering to block overseas sites which contain criminal content such as child pornography and sexual violence).

173. U.S. INT'L TRADE COMM'N, RECENT TRENDS IN U.S. SERVICES TRADE 2009 ANNUAL REPORT xi (2009), *available at* http://www.usitc.gov/publications/332/pub4084.pdf.

174. *Id*.

175. *Id*.

less true for e-services than it is for traditional services. Indeed, if anything, the correlation is probably stronger in the realm of e-services as the U.S. provides most of the Internet's major e-service providers such as Google, Wikipedia, Facebook, Twitter, LinkedIn, and many of the most popular blog hosting sites. In the *U.S.– Gambling Services* case the U.S. found itself in the somewhat unique position of importing an Internet service: Internet gambling. Given language barriers between the U.S. and other prominent software producers, combined with the already prominent position of U.S. companies in most e-service arenas, it seems unlikely that the U.S. will find itself an importer of a similarly lucrative service as Internet gambling.

Second, the *U.S.-Gambling Services* case was unique because U.S. Internet filtering efforts, directed at financial intermediaries, resulted in a near total denial of market access by services from a specific foreign country.[176] Currently, no filtering efforts by the U.S. government create a similarly extensive market access barrier in a given sector. Even in those sectors of Internet where the U.S. government imposes the most stringent controls, *i.e.* in the arena of access by minors to obscene materials, access is only limited in public school and libraries that wish to receive E-rate funding.[177] The barrier to market access is far from complete. Children can still access obscene materials at home, in Internet cafes, and on computers at public schools and libraries that prefer not to censor the Internet in exchange for discounted access to technology. Furthermore, the FCC does not require participation in the E-rate program.[178] As a result, the rarity of the circumstances that led to the *U.S.-Gambling Services* decisions combined with the entrenched and growing resistance to Internet filtering in the U.S. in all but the most universally accepted arenas, suggests that the U.S. is unlikely to find itself in violation of e-commerce related GATS commitments again.

Furthermore, the *U.S.-Gambling Services* case was unique because a regulation specifically prohibited the provision of a service by a foreign

176. Press Release, Office of New York State Attorney General, Ten Banks End Online Gambling with Credit Cards, (Feb. 11, 2003), http://www.ag.ny.gov/media_center/2003/feb/feb11b_03.htmlhttp://www.oag.state.ny.us/press/2003/feb/feb11b 03.html (Spitzer commenting that "[t]The vast majority of credit card issuers – and all issuers doing significant business with New York consumers – have now recognized their legal, ethical, and business obligation to block credit card transactions identified as online gambling.").

177. *The E-Rate: an Overview*, EDUC. & LIBRARY NETWORKS COALITION, http://www.edlinc.org/get_facts.html (last visited Feb. 7, 2011) (showing which schools and libraries and what services are being funded by the E-rate and indicating the level of participation in the E-rate program by state).

178. *E-Rate Program Discounted Telecommunications Services*, U.S. DEP'T OF EDUC., http://www2.ed.gov/about/offices/list/oii/nonpublic/erate.html (last visited Feb. 7, 2011) ("Non-profit private schools — along with public schools, and libraries — *can* receive discounted telecommunications services through the E-rate program.") (emphasis added).

supplier while allowing domestic suppliers access to the market. Given the limited nature of U.S. filtering efforts combined with the fact that most services are supplied by U.S. suppliers, this situation is not likely to repeat itself. For example, in the case where the U.S. Marine Corps has chosen to block access to social media sites, GATS commitments would not be applicable because the service targeted is a domestically supplied service and there is no disparate treatment on the basis of country of origin of the service. While the situation is somewhat more complicated when one considers AT&T's blocking of 4chan.org because AT&T was blocking a foreign website, it would nonetheless be difficult for 4chan.org to show that AT&T would not behave in a similar fashion if a U.S. based website began sending denial of service attacks to its customers.

Given that U.S. Commitments made under the GATS Agreement are unlikely to provide successful remedies for any sporadic filtering efforts that the U.S. might elect to engage in, what remedies could potential victims pursue? For filtering against U.S. based service suppliers, the best remedies are likely to be found in tort law.

V. TORT REMEDIES

Given that the WTO GATS Agreement is unlikely to provide effective remedies for those feeling the effects of Internet filtering, those affected must look elsewhere to protect their business interests. And while the U.S. government is not likely to become increasingly involved in content filtering because of First Amendment concerns among others, the potential for U.S. companies to filter the Internet as appliancization of the Internet increases is growing. One potential avenue for effective remedies to Internet filtering conducted by private actors is found in common law tort doctrine, specifically the tort of intentional interference with contractual relations and at-will relations.

A. Intentional Interference With An Existing Contract

To see how the tort of intentional interference with contractual relations would apply in the Internet filtering context, imagine a situation in which an ISP chooses to block Skype services, while allowing its own proprietary version of VoIP software to flow unimpeded to its subscribers.[179] This class of situation seems increasingly likely to occur in light

179. It is important to note that in this example the entity doing the Internet filtering is a private entity rather than the U.S. government. Also, the private entity is not filtering at the direction of the U.S. government but rather to serve its own private ends. As such, concerns of government immunity are not implicated.

of the D.C. Circuit's decision in *Comcast Corp. v. FCC*.[180] That case arose out of Comcast's network management policies that blocked subscribers from sharing files using peer-to-peer network applications, such as BitTorrent, eDonkey and Gnutella.[181] The D.C. Circuit held that the FCC does not have the authority to regulate an ISPs network management policies, as they pertain to blocking customers use of peer-to-peer network applications.[182] Thus, at least as the law stands now, the FCC is largely powerless to stop ISPs from blocking content, provided it is justified as necessary for network management.[183]

Most states recognize the common law tort of intentional interference with an existing contract as well as a tort for interference with prospective business relationships.[184] The Restatement (Second) of Torts § 766 defines intentional interference with the performance of a contract by a third person as:

> One who *intentionally* and *improperly* interferes with the performance of a contract (except a contract to marry) between another and a third person by inducing or otherwise causing the third person not to perform the contract, is subject to liability to the other for the pecuniary loss resulting to the other from the failure of the third person to perform the contract.[185]

Applying the language of the Restatement to the Skype scenario above the ISP would be the party interfering with the performance of a contract between Skype and the consumer of Skype services who is also an ISP subscriber. Thus, in order to be found liable the consumer would need to show that the ISP acted both "intentionally" and "improperly."

The first prong of the test, intentionality, is not hard to satisfy. All that is required under the Restatement (Second) of Torts § 8A is that the defendant had the purpose to cause the consequences of his act or the

---

180. Comcast Corp. v. FCC, No. 08-1291, 2010 U.S. App. LEXIS 7039 (D.C. Cir. Apr. 6, 2010).

181. Peter Svensson, *Comcast Blocks Some Internet Traffic: Tests Confirm Data Discrimination by Number 2 U.S. Service Provider,* MSNBC.COM (Oct. 19, 2007, 9:36 AM), http://www.msnbc.msn.com/id/21376597/ns/technology_and_science-internet/.

182. Comcast Corp., 2010 U.S. App. LEXIS 7039 at 54.

183. While this decision is unlikely to be the final word on the FCC's ability to regulate ISPs network management policies, it is worth noting that this challenge alone took approximately two and a half years to resolve; during which time the company's whose Internet traffic was being blocked would suffer substantial economic harm if a preliminary injunction was not obtained.

184. *See e.g.,* DAN B. DOBBS & ELLEN M. BUBLICK, CASES AND MATERIALS ON ADVANCED TORTS: ECONOMIC AND DIGNITARY TORTS BUSINESS, COMMERCIAL AND INTANGIBLE HARMS, 369-70 (2006); James O. Pearson, Jr., Annotation, *Liability for Interference with At Will Business Relationship*, 5 A.L.R. FED. 9 (2010); Joel E. Smith, *Liability of Third Party for Interference with Prospective Contractual Relationship Between Two Other Parties*, 6 A.L.R. FED. 195 (2010).

185. RESTATEMENT (SECOND) OF TORTS § 766 (emphasis added).

defendant believed that the consequences of his act were substantially certain to follow. Courts applying this standard have rejected the argument that only a purpose or desire to cause interference is sufficient to meet the intentionality requirement.[186]

To satisfy the intentionality standard it is necessary to prove the ISP had knowledge of the contractual relationship.[187] In order to successfully block Skype packets, the ISP has to inspect the packets being transmitted to determine they are Skype packets. Thus, it is reasonable to assume that there would not be Skype packets being transmitted unless there was a contractual relationship.

It was not always the case that the plaintiff was required to show both intentionality and impropriety. Historically, it was sufficient for a third-party to prove intentional interference.[188] Currently, the Restatement and courts have indicated that certain interferences in contractual relations are justifiable and thus privileged.[189] Moreover, courts are increasingly placing the burden of showing improper interference on plaintiffs.[190]

The second prong of the test, the improper interference element, is not as easily satisfied as the intentionality standard. It is easier to make the improper showing if the act of interfering with the contract also violates a pre-existing independent duty, such as a tort duty or fiduciary duty.[191] For example, in *Northeast Women's Center, Inc. v. McMonagle*, plaintiff, a women's health center, sued defendants, anti-abortion protestors, for intentional interference in contractual relations and civil RICO violations.[192] The court held that the RICO statute applied to the protesters intimidating behavior and used the evidence of RICO violations as evidence that the protestors had violated an independent duty, thereby satisfying the improper element of the intentional interference in contractual relations claim.[193]

However, in the context of Internet filtering it is unlikely that an ISP will have committed an independent tort. Consequently, plaintiffs must show that the ISPs actions were wrongful, either in terms of their

186. Kor. Supply Co. v. Lockheed Martin Corp., 63 P.3d 937, 949-50 (Cal. 2003).

187. DOBBS & ELLEN M. BUBLICK, *supra* note 184, at 370-72.

188. Lumley v. Gye, (1853) 118 Eng. Rep. 749.

189. DOBBS & ELLEN M. BUBLICK, *supra* note 184, at 370.

190. *Id*.

191. *Id*. at 374 (citing Ne. Harbor Golf Club, Inc. v. Harris, 661 A.2d 1146 (Me. 1995); Ne. Women's Ctr., Inc. v. McMonagle, 868 F.2d 1342 (3d Cir. 1989)).

192. Ne. Women's Ctr., 868 F.2d at 1345.

193. *Id*. at 1347-48 (noting that the plaintiffs "pleaded and proved that Defendants embarked on a willful campaign to use fear, harassment, intimidation and force against the Center through targeting its employees so that they would, and some did, sever their employment at the Center.").

motive or means, even though no pre-existing duty was violated.[194] Wrongful motive or means is an amorphous standard, but one court has commented that "[i]mproper means includes not only tortious behavior, but any 'predatory' behavior, including behavior that is wrongful based on an established standard of a trade or profession."[195]

A plaintiff could argue that Internet filtering that violates the principle of net neutrality violates an established standard of Internet conduct. Net neutrality is generally understood to mean a "mandate . . . prohibit[ing] network owners from discriminating against particular applications and content providers."[196] Thus, net neutrality would prohibit an ISP from prioritizing its VoIP service over Skype. This line of argument would satisfy the requirement that the action satisfied the wrongful motive or means requirement of the improper interference element of the tort of intentional interference in contractual relations.

If the Internet filtering was not discriminatory in nature between services of a similar nature, a plaintiff could still succeed on an interference in contractual relations theory if they could satisfy the multifactor test applied by courts to determine whether the interference was "improper:"

> (a) the nature of the actor's conduct, (b) the actor's motive, (c) the interests of the other which with the actor's conduct interferes, (d) the interests sought to be advanced by the actor, (e) the social interests in protecting the freedom of action of the other, (f) the proximity or remoteness of the actor's conduct to the interference, and (g) the relations between the parties.[197]

A secondary question is whether actual breach of the contract is even required for a potential plaintiff to succeed. This is relevant in the Internet filtering context because often content will not be 100% blocked. It is not necessary to block content 100% of the time in order for Internet filtering to be effective.[198] Imagine a scenario in which an ISP instead of blocking Skype traffic just slowed Skype traffic down considerably. Would that kind of filtering still be actionable as a common law tort? Although less widely accepted than § 766, § 766A of the Restatement (Second) of Torts on Intentional Interference with Another's Performance of His Own Contract provides that actual breach is not required for a potential plaintiff to succeed. The Restatement only requires that the

194. DOBBS & ELLEN M. BUBLICK, *supra* note 184, at 374.

195. Bogle v. Summit Inv. Co., LLC, 107 P.3d 520, 528-29(N.M. Ct. App. 2005).

196. Tim Wu & Christopher Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FED. COMM. L.J. 575, 575 (2007).

197. DOBBS & ELLEN M. BUBLICK, *supra* note 184, at 374 (citing Hill v. Winnebago Industries, Inc., 522 N.W.2d 326, 328-29 (Iowa Ct. App. 1994)).

198. GOLDSMITH & WU, *supra* note 27, at 67.

performance be made "to be more expensive or burdensome."[199]

To date, this author has only found one case where the plaintiff has successfully pled intentional interference in contractual relations in the Internet filtering context: *CAT Internet Services, Inc. v. Magazines.com Inc.*, 2001 U.S. Dist. LEXIS 8 (E.D. Pa. Jan. 4, 2001).[200] In *CAT* the plaintiff and defendant were Internet and e-commerce companies with interests in domain names that were very similar to one another: the plaintiff owned and operated www.magazine.com (singular), while the defendant owned and operated www.magazines.com (plural).[201] The plaintiff's website marketed electronic magazines, but at approximately the same time as suit was brought, the plaintiff was in the process of entering into agreements with third-parties, such as E-News and Magazine Mall, to market conventional magazines.[202] The defendant's website had always marketed conventional magazines.[203] The law suit originated when plaintiff discovered that the defendant was utilizing plaintiff's domain name to redirect traffic to its own website.[204] Among other claims the plaintiff brought a claim alleging both interference with contractual relations and interference with prospective contractual relations.[205]

The court considered both the prospective and actual contractual relations claims.[206] With regard to the prospective contractual relationship the court found that the plaintiff had produced sufficient evidence to survive the motion to dismiss.[207] The court stated that the plaintiff had sufficient "evidence of a prospective contractual relation between Plaintiff and E-News, Magazine Mall, and other parties, intent by the Defendant to harm the Plaintiff by preventing these relationships from occurring in the absence of a privilege or justification, and the occurrence of $100,000 in damages to the Plaintiff as a result."[208] Applying the

199. RESTATEMENT (SECOND) OF TORTS § 766A (1979).

200. *See generally* Vulcan Golf, LLC v. Google Inc., 552 F. Supp. 2d 752 (N.D. Ill. 2008). The plaintiffs pled intentional interference in current business relationship but did not provide any facts establishing the existence of a contract so the court treated the claim as one for intentional interference in prospective business relationship, which is addressed in the next section. *Id.*

201. CAT Internet Servs. Inc. v. Magazines.com Inc., No. 00-2135, 2001 U.S. Dist. LEXIS 8, at *2 (E.D. Pa. Jan. 4, 2001).

202. *Id*. at *2-3.

203. *Id*.

204. *Id*. at *3. The opinion does not provide any detail regarding how the defendant was able to redirect the Internet traffic, stating only that the plaintiff "discovered that the Defendant was utilizing CAT's domain name to redirect Internet traffic to Defendant's web site." *Id.* The pleadings are not available electronically through PACER.

205. *Id*. at *8.

206. *Id*. at *8-9.

207. *CAT Internet Servs. Inc*. v. Magazines.com Inc., 2001 U.S. Dist. LEXIS 8, at *10-11.

208. *Id*. at *11 (internal citations omitted).

same reasoning, the court found that the plaintiff's claim for interference in contractual relations also survived the motion to dismiss.[209]

The *CAT* case demonstrates that courts are willing to apply the tort of interference in contractual relations to the Internet filtering context. The parties in the *CAT* case could easily be substituted such that the plaintiff was Skype, the defendant the preferentially blocking ISP, and the third-party was the Skype customers rather than E-News and Magazine Mall. Such a substitution illustrates that such cases, if properly pled, can survive the motion to dismiss stage and constitute at least a colorable claim for relief. However, the case did not proceed to trial. The case was dismissed with prejudice pursuant to Fed. R. Civ. P. 41(a)(1) approximately three months prior to its scheduled trial date.[210]

One other case, *Verizon Advanced Data, Inc. v. Frognet, Inc.*,[211] further demonstrates that plaintiffs will likely be able to succeed on interference in contractual relation claims in the context of the Internet, even if they are only able to present circumstantial evidence to satisfy the improper element of the tort. Verizon supplied Internet bandwidth to FrogNet under a contract. In late 2002, Verizon told FrogNet that it could no longer add new customers unless it made certain equipment upgrades. As a result of this action FrogNet claimed it lost 180 customers and brought claims against Verizon for intentional interference with its business relationship with those customers.[212] Verizon moved for summary judgment on that claim, but the court rejected Verizon's motion.[213] The court specifically noted that FrogNet had provided substantial circumstantial evidence showing that "Verizon may have been attempting to keep FrogNet from growing while another Verizon entity – Verizon Online – was about to begin providing DSL service,"[214] which satisfied the requirement that the interference be improper.

Conversely, in *Asch Webhosting, Inc. v. Adelphia Business Solutions Investment, LLC*,[215] the Third Circuit found that the plaintiff's circum-

209. *Id*. at *14 (citing the same factors for the actual contractual relationship as it did for the prospective contractual relationship).

210. It appears the case was dismissed because the plaintiff's insurance company stopped paying to prosecute the case. CAT Internet Servs.Inc. v. Providence Wash.Ins. Co., 333 F.3d 138, 140 (3d Cir. 2002) (explaining that after CAT was sued in Tennessee by Magazines.com, CAT's "insurers, Providence Washington and York, declined to undertake their defense under the advertising injury provisions of their standard commercial liability policies.").

211. Verizon Advanced Data, Inc. v. Frognet, Inc., No. 2:05-cv-955, 2010 U.S. Dist. LEXIS 32595 (E.D. Oh. Apr. 2, 2010).

212. *Id*. at *8-9.

213. *Id*. at *24.

214. *Id*. at *10.

215. Asch Webhosting, Inc. v. Adelphia Business Solutions Inv., LLC, No. 09-2296, 2010 U.S. App. LEXIS 1546 (3d Cir. Jan. 25, 2010).

stantial evidence was lacking. Asch purchased Internet bandwidth from Adelphia under a contract that was later terminated by Adelphia, after Adelphia received complaints about e-mails emanating from Asch's IP addresses.[216] Asch sued Adelphia for intentional interference with contractual relations.[217] The Third Circuit upheld the district court's grant of summary judgment in favor of Adelphia finding that there was no interference.[218] However, in finding in favor of the defendant, the Third Circuit relied on an exculpatory clause in the contract between Asch and Adelphia that released Adelphia from "all liability or responsibility for any direct, indirect, incidental or consequential damages, suffered by [Asch] in connection with [its] use of or inability to use the [Adelphia] internet services."[219]

In its reasoning, the Third Circuit commented on the standard necessary to prove predatory behavior, which is one of the ways a plaintiff may satisfy the "improper" element of the tort. Asch argued that Adelphia's breach of contract was predatory and pointed to e-mails implying that Adelphia had breached the contract to ensure Asch did not increase the number of IP addresses it required.[220] Rejecting Asch's argument, the Third Circuit said "Asch [had] not presented evidence suggesting that [Adelphia] had a reason, other than the explanations it gave [concerning the complaints related to Asch's IP addresses], for terminating its services to a paying client."[221] Had Asch presented a more complete allegation that Adelphia's breach of contract was explicitly to prevent Asch's growth, as FrogNet did, it seems possible that the Third Circuit would have found Adelphia's actions constituted predatory behavior. Hence, the Third Circuit's decision in *Asch Webhosting* does not preclude recovery for intentional interference in contractual relations, as Asch did not present sufficient circumstantial evidence of improper action on the part of Adelphia.

VI. INTERFERENCE WITH AT-WILL RELATIONSHIPS

What happens in those cases where there is no contractual relationship, such as in the case where a website that doesn't provide a contractual service, but merely provides content, is simply blocked as a result of Internet filtering? This situation appears to fit within the tort of interference with an at-will relationship, which is almost universally ac-

216. *Id.* at *2.

217. *Id.* at *1.

218. *Id.* at *10.

219. *Id.* at *6 (emphasis added).

220. *Id.* at *7.

221. Asch Webhosting, 2010 U.S. App. LEXIS 1546 at *7.

cepted.[222] The tort requires proof of the following elements: "the existence of a business relationship or expectancy, it often being stated that an existing contract is not required; knowledge by the interferer of the relationship or expectancy; an intentional act of interference; proof that the interference caused the harm sustained; and damage to the plaintiff."[223] Once the plaintiff establishes the required elements the burden shifts to the defendant to demonstrate that his or her actions were justified.[224]

At least one case, in Illinois, has considered the tort of interference with an at-will business relationship in the Internet context. In *Vulcan Golf, LLC v. Google Inc.*,[225] the plaintiffs alleged that the defendant's registered domain names that are the same or substantially similar to plaintiff's distinctive trade names and marks. The defendants behaved this way in order to generate advertising revenues at the expense of the plaintiffs. When an Internet user, upon seeing the similar domain name, became confused and selected the wrong website, the defendants generated ad revenue.[226] The plaintiff further alleged that Google partnered with the defendants, who have hundreds of similar domain names under its control, by helping the defendants select and place ads on the similar domains.[227]

Although the court has yet to reach a complete resolution of the case, the court has denied the defendants' motion to dismiss the intentional interference with prospective business advantage claim. The court rejected the defendants' position that the plaintiffs failed to assert "a business expectancy with a specific third-party as well as particular action by the defendant directed towards that third-party" because the plaintiffs' contention that they "would have done business with a third-party class of "Internet users/consumers" [was] too conclusory" to "raise the plaintiffs' right to relief above the speculative level."[228] Instead, the court found that "identification of general classes of third-parties (here, Internet users) can be sufficient" to survive a motion to dismiss because "[t]he court is simply not willing at the motion to dismiss stage to definitively state that such a showing, while likely a daunting task, is impossible such that the plaintiffs cannot state a claim."[229]

---

222. James O. Pearson, Jr., Annotation, *Liability for Interference with At Will Business Relationship*, 5 A.L.R. FED. 9 at §2[a] (2010).

223. *Id.* (internal citations omitted).

224. *Id.*

225. Vulcan Golf, LLC v. Google, Inc., 552 F. Supp. 2d 752 (N.D. Ill. 2008).

226. *Id.* at 759-60.

227. *Id.* at 760.

228. *Id.* at 760, 781.

229. *Id.* at 781 (citing Cook v. Winfrey, 141 F.3d 322, 328 (7th Cir. 1998)).

The Seventh Circuit has previously held, in the non-Internet context, that under Illinois law it is sufficient for a plaintiff to identify a "class" of third-parties with whom he or she might have had a prospective business relationship, rather than a specific single third-party.[230] In *Cook v. Winfrey*, the plaintiff sued Oprah Winfrey for interfering with his ability to publish tabloid stories regarding her alleged drug abuse.[231] The plaintiff identified "the media" as the third-party class with whom he had a prospective business relationship and the Seventh Circuit, reversing the district court's ruling, found that this was more than is required under notice pleading standards and thus sufficient to survive a motion to dismiss.[232] Consequently, it seems possible that given the right evidence a plaintiff could win on the basis of intentional interference with a prospective business advantage claim, even if the plaintiff could do no more than identify a class of prospective customers, such as Internet users.

VII. CONCLUSION

Internet filtering is a growing concern worldwide. The number of countries filtering the Internet has increased from "a handful" just under a decade ago to approximately 40 in 2010.[233] While actors in the United States do not carry out extensive content based Internet filtering, they do engage in some actions, such as AT&T's recent blocking of 4chan.org. The potential for ISPs to impose restrictions on services such as VoIP phone service or for cell phones carriers to restrict the ways in which phones can browse the Internet is ever present, and growing if one accepts Zittrain's appliancization theory.

The remedies available under the WTO GATS Agreement are, however, unlikely to be available or effective for U.S. actors' future attempts at Internet filtering. The *U.S.-Gambling Services* decision, in which the U.S. was found in violation of its WTO GATS Commitments, is unlikely to be repeated in part because of the limited amount of nationality based discriminatory filtering the U.S. government conducts and in part because of the unique circumstances that combined in the *U.S.-Gambling*

230. Cook v. Winfrey, 141 F.3d 322, 328 (7th Cir. 1998) (citing River Park, Inc. v. City of Highland Park, 667 N.E.2d 499, 507 (Ill. App. Ct. 1996); Parkway Bank & Trust Co. v. City of Darien, 357 N.E.2d 211, 214, (Ill. App. Ct. 1976)).

231. Cook, 141 F.3d at 324.

232. *Id.* at 328.

233. Javier C. Hernandez, *Google Official Calls for Action on Web Limits*, N.Y. TIMES, Mar. 24, 2010, http://www.nytimes.com/2010/03/25/technology/25google.html?hpw; *Google and Internet Control in China: A Nexus Between Human Rights and Trade?: Hearing Before the Cong.-Exec. Comm'n on China*, 111th Cong. (2010) (statement of Alan Davidson, Director of Public Policy, Google Inc.), *available at* http://www.cecc.gov/pages/hearings/2010/20100324/davidsonTestimony.pdf?PHPSESSID=1e18ee1fbf60adabafcd336342f0235e.

Services case. As a result, those facing the effects of filtering by private actors would likely have more success by pursuing common law tort remedies, such as intentional interference in a contractual relationship or intentional interference in an at-will relationship. In the context of contractual relationships, a growing body of precedent suggests that claims for interference in contractual relations as a result of Internet filtering are at least colorable claims, if not likely to be successful ultimately. Additionally, at least one court has considered this tort in the context of a prospective at-will relationship and found that alleging harm to a class of third-party users consisting of Internet users is sufficient to survive a motion to dismiss; however, whether further success is possible remains to be tested.