Brigham Young University International Law & Management Review

Volume 1 | Issue 1 Article 9

8-16-2005

The World Summit on the Information Society: Making the Case for Private Industry Filtering to Control Extraterritorial Jurisdiction and Transnational Internet Censorship Conflicts

Jay Wahlquist

THE WORLD SUMMIT ON THE INFORMATION SOCIETY: MAKING THE CASE FOR PRIVATE INDUSTRY FILTERING TO CONTROL EXTRATERRITORIAL JURISDICTION AND TRANSNATIONAL INTERNET CENSORSHIP CONFLICTS

I. INTRODUCTION

Creators of internet content and corporations that utilize internet portals internationally should be aware of two issues that will come before the World Summit on the Information Society (WSIS) this November. The first issue is unlawful content and the second is access protection. This note explores the manner in which various countries plan on handling these issues.[1] The conclusions reached at the WSIS may affect what is accessible on the Internet, and if content creators will be liable for violating foreign laws in various jurisdictions simply for publishing certain materials on the Internet.

This paper specifically addresses foreign assertion of jurisdiction over Internet content creators and proposes means to avoid the chilling effect foreign assertion of jurisdiction inevitably has on speech and Internet based commerce. Part II of this paper provides a brief background on both the WSIS and the Working Group on Internet Governance (WGIG), and outlines the problems

---

[1] *See* Working Group on Internet Governance, *Issue Paper on Unlawful Content and Access Protection*, *available at* http://wgig.org/docs/WP-UnlawfulContent.pdf (last visited Mar. 19, 2005). "'Unlawful content' refers to content that is deemed illegal. That is, the origination, production, and sometimes even consumption, of the content can result in prosecution and conviction in a court of law. 'Access protection' refers to the partial or complete denial of access on the grounds that the content may be illegal, exploited for criminal ends, or potentially harmful. Such denial may be necessary to protect end-users (such as children), potential victims, or even content intermediaries such as Internet service providers." *Id.* § 1.

created by the widely used effects-based jurisdiction. Part III discusses the three[2] main alternatives for conferring jurisdiction over Internet content and regulating access: (1) effects-based jurisdiction, (2) target-based jurisdiction, and (3) private industry filtering. Finally, Part III also analyzes how well each method balances governmental law enforcement interests against the interests of individual free speech and explains why the WGIG and the WSIS must adopt private industry filtering as the preferred method for dealing with Internet jurisdiction.

II. BACKGROUND

The World Summit on the Information Society is "held under the high patronage of the UN Secretary-General, with [the International Telecommunication Union (ITU)] taking the lead role in preparations."[3] The WSIS convened because "world leaders decided that a global vision and a global dialogue were needed to build the framework of an all-inclusive and equitable Information Society."[4]

---

[2] In reality, there are more than three alternatives to address the problem of Internet jurisdiction. For example, it has been proposed that an international organization should be created which would regulate the Internet. *See* John Zarocostas, *U.N. Group Seeks Control of Internet*, COMPUTER CRIME RESEARCH CENTER, Nov. 18, 2003, *at* http://www.crime-research.org/news/2003/11/Mess1802.html (last visited Mar. 8, 2005). However, the viability of this solution is questionable as it faces strong opposition from some free-market nations. *Id.* Additionally, due to "the broad differences in culture and law, it is extremely difficult to come to an objective judgment on whether some content is acceptable or unlawful." Working Group on Internet Governance, *Issue Paper, supra* note 1, at 1. Finally, it is not clear if such an organization would eventually address the issue of speech or stick to areas of relative universal agreement such as fraud. Therefore, while other solutions exist, only the three solutions, which, in the opinion of the author, are most probable, will be discussed.

[3] International Telecommunication Union, *Background and Origins of the Summit*, *at* http://www.itu.int/wsis/basic/background.html (last visited Mar. 19, 2005).

[4] International Telecommunication Union, *Frequently Asked Questions — 6.1 Why is there a World Summit on the Information Society?*, *at* http://www.itu.int/wsis/basic/faqs.asp (last visited Mar. 19, 2005).

The WSIS consists of two chronological phases; the first was completed in Geneva during December, 2003.[5] As part of the first phase, the WSIS requested the establishment of a Working Group on Internet Governance (WGIG).[6] The WGIG's duty is "to investigate and make proposals for action ... on governance of the Internet," which will be considered in the second phase of the WSIS set to take place November 16–18, 2005 in Tunisia.[7]

Two issues identified by the WGIG thus far, unlawful content and access protection,[8] are currently on the WSIS agenda. Thus, the WGIG and the WSIS provide the perfect opportunity to address and deal with global Internet jurisdiction problems and more specifically, the problems arising from effects-based jurisdiction. The opportunity is timely, as effects-based jurisdiction is quickly becoming the primary method employed for determining proper jurisdiction.[9]

Effects-based jurisdiction allows for exercise of jurisdiction whenever one element of a crime is committed in the forum state.[10] It is not necessary that all of the elements be committed in one forum.[11] Under the effects-based

---

[5] International Telecommunication Union, *Background*, *supra* note 3.

[6] World Summit on the Information Society, *Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, *U.N. Doc.* WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003), *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html (last visited Apr. 26, 2005).

[7] *Id.*; International Telecommunication Union, *Background*, *supra* note 3.

[8] *See* Working Group on Internet Governance, *Issue Paper*, *supra* note 1.

[9] Michael Geist, *The Legal Implications of the Yahoo! Inc. Nazi Memorabilia Dispute: An Interview with Professor Michael Geist*, JURISCOM.NET, Jan. 18, 2001, *at* http://www.juriscom.net/en/uni/doc/yahoo/geist.html (last visited April 26,2005) [hereinafter Geist, *Nazi Memorabilia Dispute*] (interviews with Michael Geist organized by Lionel Thoumyre).

[10] Ray August, *International Cyber-jurisdiction: A Comparative Analysis*, 39 AM. BUS. L.J. 531, 536 (2002).

[11] *Id.* at 537.

analysis, a court has jurisdiction when that jurisdiction feels the negative effects or harm from the action.

Various cases use an effects-based analysis to assert jurisdiction over Internet related content.[12] In particular, the United States uses this analysis to assert jurisdiction over foreign entities in cases involving fraud and child pornography.[13] These cases go unnoticed because censorship of child pornography and fraud are areas of near universal agreement.[14] However, the story is quite different when courts use effects-based analysis to assert jurisdiction to censor content that does not enjoy similar universal agreement. International attempts to regulate Internet content and online commerce will suffer from the contradictory standards and conflicting judicial rulings of diverse international jurisdictions. Additionally, Internet content creators may face criminal charges in foreign nations even though the offending content is legal in their own country.[15] Accordingly, content providers, fearing lawsuits, will refrain from posting content on the Internet despite being legally sanctioned or protected in their localities. Consequently, effects-based jurisdiction schemes threaten to restrain e-commerce and ultimately chill free speech. This chilling effect will be illustrated more fully by analyzing the effects-based jurisdiction utilized in the French case *UEJF and Licra v. Yahoo! Inc. and Yahoo France* (*Yahoo!*).[16]

---

[12] *Id.* at 537–38.

[13] Mathew Fagin, Comment, *Regulating Speech Across Borders: Technology vs. Values*, 9 MICH. TELECOMM. & TECH. L. REV. 395, 449 (2003).

[14] *Id.*

[15] Working Group on Internet Governance, *Issue Paper*, *supra* note 1, at 1.

[16] UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, May 22, 2000, N° RG: 00/05308, obs. C.Bensoam & J.Gomez, *translation available at* http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (last visited Apr. 26 2005).

III. Three Alternative Methods

A. Effects-based Jurisdiction

The French case *UEJF and Licra v. Yahoo! Inc. and Yahoo France* effectively illustrates the problems inherent in effects-based jurisdiction schemes. *Yahoo!* demonstrates how an effects-based analysis unduly grants foreign courts jurisdiction over virtually all Internet content. Moreover, it illustrates how wide-sweeping jurisdiction creates conflicts in determining what is legal to post on internationally accessible Internet sites.

In *Yahoo!*, a French court found Yahoo! Inc. guilty of violating French law that prohibits the display of Nazi memorabilia.[17] Although Yahoo! Inc. clearly had no intention of violating French law and the Nazi memorabilia represented a marginal portion of the content available on its broadly inclusive auction site, in May 2000, the French judge deemed French courts as competent to preside over the dispute because Internet surfers in France suffered damage.[18] The French Interim Court affirmed the decision on similar grounds. That court concluded that although Yahoo!'s auction site is generally directed at users in the United States, as evidenced by the terms of delivery, language, currency, and methods of payment used, the sale of Nazi memorabilia could not be considered as directed only at U.S. consumers because it "may be of interest to any person."[19] Thus, according to the French Interim Court, the mere fact that harm

[17] *Id.*

[18] *Id.*

[19] UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, Nov. 20, 2000, N° RG: 00/05308, obs. J.Gomez, *translation available at* http://www.cdt.org/speech/international/001120yahoofrance.pdf (last visited Mar. 5, 2005).

was felt in France and the fact that Yahoo! Inc. had at least some ability to determine a user's origin were enough to grant the French court competent jurisdiction.[20]

The French Interim Court's assertion of jurisdiction created a large public outcry,[21] particularly in the United States. This outcry is rooted in the possibility that other countries will adopt the dangerous precedent set by the French Interim Court's decision to assert foreign jurisdiction in speech related cases that affect international commerce.[22] Opponents of effects-based jurisdiction stress that it will lead to "a jurisdictional morass, an overabundance of jurisdictional claims, and an undesirable increase in the cost of online publication."[23]

It is important to note that the French case did not regulate the sale of Nazi items, which more traditional methods would typically regulate. Rather, the *Yahoo!* ruling focused specifically on the mere display of Nazi memorabilia.[24] If other countries adopt the *Yahoo!* court's rationale, any country with Internet access will assert jurisdiction over all content on the Internet because potentially objectionable material may have been displayed in that country.[25] This will inevitably lead to contradictory standards and judicial rulings, as each country attempts to regulate Internet content regardless of its origin or directed

---

[20] *Id.*

[21] Geist, *Nazi Memorabilia Dispute*, *supra* note 9.

[22] *Id.*

[23] Fagin, *supra* note 13, at 407.

[24] Ben Laurie, *An Expert's Apology*, APACHE-SSL.ORG, Nov. 21, 2000, *at* http://www.apache-ssl.org/apology.html (last visited Mar. 7, 2005).

[25] Fagin, *supra* note 13, at 410-11.

audience.[26] In fact, a U.S. District court has already refused to enforce the French decision in the U.S.,[27] legitimizing critics' fears that inconsistent rulings will provide additional compliance costs and impact content providers' cost-benefit analyses.

The logical extension of the *Yahoo!* rationale is that every internet publishing entity will be forced to implement and "maintain a huge matrix of pages versus jurisdictions to see who can and can't see what."[28] The cost and effort seem pointless or frivolous when one considers the ease with which filtering technology can protect various Internet users.[29] Nevertheless, even if filtering technology is effective, how will online content providers know whether they are violating laws in countries all over the world? Will corporations be required to hire lawyers in each nation to inspect every piece of questionable material? Conversely, must entities refrain from publishing material that is questionable by any stretch of the world's collective imagination? By using international content filtering,[30] content providers may avoid potential liability and online content censorship, but such a course will aggregate into a global chilling effect on speech and online commerce.

Support for the fear of a chilling effect can be found in Yahoo!'s response to the French decision and CompuServe's response to a similar situation

---

[26] Rinat Hadas, Case Comment, *International Internet Jurisdiction: Whose Law is Right?*, 15 FLA. J. INT'L L. 299, 307 (2002).

[27] Yahoo!, Inc. v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

[28] Laurie, *supra* note 24.

[29] *Id.*

[30] Fagin, *supra* note 13, at 414–15.

involving Germany in 1995.[31] In both cases, the Internet service provider blocked the offensive content rather than spend resources implementing centralized, nation-specific filters.[32] Extraterritorial restriction of speech, conflicting laws, and increased costs of Internet publication all bolster the fears and criticisms of effects-based jurisdiction.[33]

Some, however, argue that fears of effects-based jurisdiction are unfounded. For example, Jack Goldsmith, professor of law at the University of Chicago Law School, posits that cyberspace transactions do not truly differ from traditional transnational transactions and can be similarly regulated.[34] He provides several examples of non-Internet related cases in which laws are applied extraterritorially with negative spillover effects.[35] He points out that while these spillover effects are the central problem of effect-based jurisdiction, they are inevitable because the social and economic cost of eliminating them is too high.[36] Therefore, the spillover effects of extraterritorial application of other countries'

---

[31] CompuServe was threatened with a lawsuit in December 1995 for allowing German CompuServe subscribers to access discussion groups containing pornographic materials in violation of German law. In response, CompuServe unilaterally blocked access to the discussion groups, effectively blocking the groups for all subscribers world-wide. Eventually, CompuServe again allowed access after making filtering technology available to their German subscribers. However, the German prosecutor notified CompuServe that such efforts were still not in compliance with German laws. Felix Somm, head of CompuServe Deutschland was subsequently given a suspended two year sentence for violation of German law. The conviction was then reversed a year later by a superior court. *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1224–25 (1998); Associated Press, *CompuServe Ex-Official's Porn-Case Conviction Reversed* (Nov. 17, 1999), *available at* http://www.cyber-rights.org/isps/somm-dec.htm (last visited Apr. 26, 2005) [hereinafter Associated Press, *CompuServe*].

[32] Goldsmith, *supra* note 31, at 1224; Marc Le Menestrel et al., *Internet E-ethics in Confrontation with an Activists' Agenda: Yahoo! on Trial*, *at* http://www.econ.upf.es/deehome/what/wpapers/postscripts/577.pdf (Nov. 2001) (last visited Apr. 26, 2005).

[33] Fagin, *supra* note 13, at 408, 414–15.

[34] Goldsmith, *supra* note 31, at 1200.

[35] *Id.* at 1211–12.

[36] *Id.* at 1212.

laws do not originate from applying national law to internationally available Internet sites.[37] The problems of extraterritorial jurisdiction and compliance existed previously, and the existing tools of modern conflict laws and technology deal with them as ably as they will with the spillover effects of extraterritorial Internet regulation.[38] Professor Goldsmith does not mean to say that laws will not change, but rather, countries can regulate Internet publication and commerce just as they regulate transnational transactions.[39]

One important fact supports Goldsmith's argument: while a country may theoretically impose its laws on the world, practically speaking, enforcement of those laws depends on the country's ability to implement them internationally.[40] A country's power to enforce its laws is tied to its ability to attach any assets the accused entity may maintain in the country.[41] However, most Internet users and online publishers do not maintain assets abroad.[42] Thus, it seems that fears of freedom of speech restraints imposed by a ruling in a foreign court have little to no practical basis.[43] Foreign rulings will primarily affect multinational corporations that maintain assets in the regulating jurisdiction.[44] Just as multinational corporations already accept liability in brick and mortar transactions they will start to include liability costs associated with associated click and mortar

---

37 *Id.*
38 *Id.* at 1213.
39 *Id.* at 1200-01, 1213.
40 *Id.* at 1216-17.
41 *Id.*
42 *Id.* at 1217.
43 *See id.*
44 *Id.*

enterprises in cost-benefit analyses prior to investing significant assets in foreign jurisdictions.[45]

The *Yahoo!* case reinforces and enhances Goldsmith's reasoning. Due to the subsequent U.S. District Court case, Yahoo! Inc. did not implement the filtering mandated by the French court.[46] Although they removed the objectionable material,[47] it is not likely that Yahoo! Inc. will implement the filtering in the near future unless they acquire direct assets in France that could be used to enforce the French ruling.[48] In summary, Goldsmith concludes that extraterritorial assertion of jurisdiction is unlikely to stifle individual or corporate online speech.[49]

Goldsmith's enforceability analysis is logical and practical for companies. However, according to the aftermath of both the Yahoo! and CompuServe cases, it is unlikely that individuals and companies will remain unaffected by court rulings. In both cases the content found on these companies' servers was not placed there by the company, but by individual users. Goldsmith briefly mentions the possibility of indirect effects on users who are dependent on service providers with a presence in the regulating jurisdiction, but he does not give it much consideration.[50] In the *Yahoo!* case, individuals sold Nazi memora-

---

[45] Fagin, *supra* note 13, at 417–18 (summarizing Goldsmith, *supra* note 31).

[46] *See* Yahoo!, Inc. v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); Hadas, *supra* note 26, at 307–08.

[47] The Associated Press & Reuters, *Yahoo! Nazi Auction Ban Welcomed* (Jan. 3, 2001), *available at* http://archives.cnn.com/2001/WORLD/europe/01/03/net.hate/ (last visited Apr. 26, 2005).

[48] *See* Le Menestrel, *supra* note 32.

[49] *See* Goldsmith, *supra* note 31, at 1217.

[50] *Id.*

bilia on Yahoo's auction website.[51] In CompuServe, individual users posted information to discussion groups.[52] Thus, the Internet Service Provider and the individual content provider were arguably distinct entities. Both companies currently state in their terms of service that the individual users will be responsible for any unlawful information posted on the Internet through their service.[53] Despite such attempts to ascribe liability for content away from the company, Yahoo! Inc. specifically changed its user agreement to prohibit Nazi memorabilia as a result of the French *Yahoo!* case.[54] Additionally, at the time of the French *Yahoo!* case, Yahoo! Inc.'s terms of service stipulated that the site was governed by the laws of the United States.[55] However, in light of the *Yahoo!* case, this type of service agreement's terms and choice of law provisions do not seem to deter courts from exercising extraterritorial jurisdiction over content providers.[56] Ultimately, these agreements and provisions offer little protection to content providers who are forced to remove objectionable material from their online portals for fear of lawsuits and possible fines.

Although individual content creators may be immune to assertions of foreign jurisdiction as Goldsmith argues, online content and portal providers are restrained through the assertion of jurisdiction over service providers. Those

---

[51] Le Menestrel, *supra* note 32, § 1.3.

[52] Associated Press, *CompuServe*, *supra* note 31.

[53] Yahoo!, *Terms of Service*, *available at* http://docs.yahoo.com/info/terms/ (last visited Mar. 7, 2005); CompuServe, *Terms of Use*, *available at* http://webcenters.compuserve.com/compuserve/menu/terms.jsp (last visited Mar. 7, 2005).

[54] Fagin, *supra* note 13, at 424–25.

[55] Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1350 (2001) [hereinafter Geist, *Is There a There There?*].

[56] *Id.* at 1406.

placing lawsuits need not go after individuals posting objectionable content. There is greater incentive to go after the companies or web portals that provide access to the information. If all major companies restrict or block objectionable material for fear of foreign lawsuits, individual expression of thought and opinion will be severely restrained as will the companies' ability to successfully operate online publication services. Online services like discussion boards, web hosting services, or auctions on sites such as Yahoo!, MSN, AOL, CompuServe, Amazon, and eBay will no longer be able to provide forums for individual expression and free speech.[57] Individuals will be left to maintain their own web server, find a lesser known company unafraid of litigation, or find a company willing to publish such information for a fee.

If there is a demand or desire for such information, it will always be found on the Internet.[58] However, part of the value in services like Yahoo! or eBay is that they are inexpensive, well known, and frequently visited. Considering the immense size of the Internet and the innumerable websites available, the greatest utility that services like eBay or Yahoo! offer is the large number of visitors that are likely to see and have ready access to the information. Thus, limiting the comprehensive scope of the services and content provided by these well-known companies will stifle the free flow of information and expression.

---

[57] In addition to the cases against Yahoo! Inc. and CompuServe, suits have been threatened against eBay.com, Amazon.com, and Barnesandnoble.com for the sale of Nazi and KKK items as well as Hitler's *Mein Kampf*. These threats have caused these retailers to either block or restrict the sale of such items despite their legality in the United States. Le Menestrel, *supra* note 32, § 1.1. *See also* Fagin, *supra* note 13, at 425 n.92; Steve Kettmann, *He Won't Join Amazon's 'Kampf'*, WIRED.COM, Dec. 2, 1999, *at* http://www.wired.com/news/print/ 0,1294,32835,00.html (last visited Apr. 26, 2005).

[58] Geist, *Nazi Memorabilia Dispute*, *supra* note 9.

The greater the number of countries that use effects-based jurisdiction, the greater the chilling effect on speech. Even though individuals may escape international litigation, the restrictions placed on companies and web servers will still inhibit freedom of expression. Therefore, for the sake of protecting free expression and transnational commerce, the WGIG and the WSIS must take steps to curb the use of effects-based jurisdiction.

B. Target-based Jurisdiction

Target-based jurisdiction is one possible alternative that seeks to avoid the negative aspects of effects-based analysis.[59] A target-based analysis attempts to identify the intent of the online content provider by considering the actions and efforts of content providers to target or not target a specific forum or audience.[60] This type of analysis provides predictability and certainty for online publishers and helps eliminate the spillover effects of an effects-based analysis as publishers may avoid jurisdictions where they wish to avoid court actions.[61]

Despite its benefits, target-based analysis is not likely to replace effects-based analysis. Courts are reluctant to use this analysis if local harm would go uncorrected when servers and websites unintended for that locality are immunized under target-based analyses.[62] Therefore, many courts are likely to

[59] Geist, *Is There a There There?*, *supra* note 55, at 1380–81.

[60] *Id.* at 1380.

[61] *Id.* at 1380–81.

[62] Fagin, *supra* note 13, at 436.

continue employing the wider reaching effects-based analysis.[63] In the case of speech and censorship, laws vary greatly from country to country.

In order for the target-based analysis to work, there must be a standard for determining when a publisher is targeting a forum.[64] A targeted relationship that subjects the individual or company to a foreign country's jurisdiction should require more certainty than an effects-based analysis.[65] Whatever the standard is, it must be technologically neutral.[66] For example, it may be appropriate today to consider the language and currency used on a particular website when determining which jurisdictions the content creator has targeted.[67] However, emerging technologies allow for real-time language and currency conversion and limit the value of such criteria for accurate target determination.[68] The targeting standard must also be content neutral to avoid favoring any interest group over another (e.g. buyers over sellers or consumers over manufacturers).[69]

One appropriate criterion for determining when a publisher is targeting a forum is foreseeability.[70] This criterion would depend upon the following factors: contracts, technology, and actual or implied knowledge.[71] Individually, none of these factors are determinative, but each is important to a proper foreseeability analysis.[72]

---

63 *Id.*
64 Geist, *Is There a There There?*, *supra* note 55, at 1384.
65 *See id.*
66 *Id.*
67 *Id.* at 1384–85.
68 *Id.*
69 *Id.* at 1385.
70 *Id.*
71 *Id.*
72 *Id.* at 1386.

First, contracts provide evidence of foreseeability as to jurisdiction; and the value of contract forum selection clauses depends on the terms of the contract as well as the manner in which the parties consent to the contract.[73] Based on U.S. court decisions, if the user is required to assent to the terms and conditions using clickable icons such as 'I agree' icons, courts are more likely to enforce these mutually agreed upon terms.[74] Courts are less likely to enforce non-consensual agreements. Thus, if the terms and conditions are merely contained on a separate page that the user can choose to read or not, the court may find no assent between the parties.[75]

Perhaps more important than the way in which parties assent to forum selection clauses is the reasonableness of the contract terms. Courts will generally weigh the forum selection clause in light of the reasonableness of the clause, the ties to the selected forum, and the laws of the selected forum. Such considerations are taken to prevent a race-to-the-bottom effect where companies try to contract into the most favorable jurisdiction despite other considerations.[76]

Incidentally, while the presence of a contract forum selection clause may enhance the ability of a court to determine the foreseeability of a targeted audience, the absence of such a clause may also allow the courts to deduce the website's intended users. Rather than a standard contract, some websites provide users with the opportunity to key in his or her jurisdiction, which information determines whether or not the website will allow the user access to its site.[77] This

---

[73] *Id.*
[74] *Id.* at 1387.
[75] *Id.*
[76] *Id.* at 1391.
[77] *Id.* at 1391–92.

type of subjective access granting based on location proves the online provider's intent to target a particular audience and restrict access in particular jurisdictions.[78] This process makes the web provider's intent more apparent; however, when prescribing jurisdiction, courts will still consider the ease with which users can circumvent such provisions in order to gain access to the site.[79]

The second factor that may determine whether or not a web provider has foreseeably targeted a particular jurisdiction is technology. As new technologies continue to emerge, websites have the ability to determine the user's geographic location with increasing accuracy.[80] Once the provider identifies the user's geographic location, the website can alter or prevent the user's access in order to avoid that particular jurisdiction. Accordingly, modern technology can constructively help courts to determine the content creator's intent to target or avoid a particular jurisdiction.

For example, some of these technologies can determine the user's location by focusing on the user's IP (Internet Protocol) address. Various proprietary products are produced to determine a user's location, many of which boast up to 99% accuracy.[81] Alternatively, other new technologies collect location information voluntarily from users, typically through attribute certificates and credit card information.[82]

---

[78] *Id.* at 1391.

[79] *Id.* at 1392.

[80] *See id.* at 1393.

[81] *Id.* at 1397.

[82] *Id.* at 1398–99. An attribute certificate is a digitally signed certificate that presents information about a particular user, such as geographic location, without providing the user's identity. The digitally signed certificates also prove difficult for other Internet users to forge. *Id.*

As online entities improve upon existing technologies and continue to develop new technologies, they will increase their accuracy in determining a user's location. Consequently, they will possess increased capabilities to allow, block, or change the content viewed by certain users, based upon the user's specific jurisdiction. When analyzing technology as a factor in the foreseeability of online providers' liability in particular jurisdictions, courts should not require online entities to use specific methods to identify a user's location but should merely consider the technologies available and used at the time.[83]

The final factor of the foreseeability test in target-based jurisdiction is actual or implied knowledge.[84] Actual knowledge of a user's location can be determined through geographic location technology, shipment of goods, receipt of contact emails, etc.[85] Courts have typically attributed implied knowledge to defendants in defamation, tort, libel, and illegal gambling cases where the offending party should have been aware of the cause of his or her actions in the targeted jurisdictions.[86] The actual or implied knowledge factor prevents companies from hiding behind contract clauses and technological screening initiatives when in fact they knew or should have known that users from a particular jurisdiction accessed their site.[87]

If target-based analyses employ foreseeability tests that include weighing the three factors discussed above, they would effectively allow online entities to

---

[83] *Id.* at 1401.
[84] *Id.* at 1402.
[85] *Id.* at 1397, 1403.
[86] *Id.* at 1402.
[87] *Id.*

predict which courts may prescribe jurisdiction over them.[88] This in turn would allow them to avoid areas that they are unprepared or unwilling to enter.[89] It would remedy the costly speech-chilling and commerce inhibiting results of effects-based jurisdiction as online entities operating under a target-based regime would know of and have the ability to control which courts would have jurisdiction over them.

However, as stated above, countries are unlikely to adopt this method if they need to rely on foreign courts to correct the harm. Until a significant number of countries articulate and accept a standard test, each country will have its own method of determining when an online provider has targeted a particular forum, making it difficult to realize the benefits of the target-based approach. Essentially, this creates the same problems already evident in an effects-based jurisdiction because jurisdictional standards are only predictable if the targeting tests are standardized internationally. Therefore, in order for the WSIS to effectively implement this method, it must accomplish the overwhelming task of both articulating an acceptable and reliable standard *and* convincing nations to forego exercising jurisdiction, even in cases where perceived and actual harms go uncorrected.

C. Private Industry Filtering

Another method of regulating Internet speech and commerce without unforeseen and unwanted extraterritorial effects is private industry filtering.

---

[88] *Id.* at 1404.

[89] *Id.*

According to this method, countries require Internet Service Providers (ISPs) or users to install software to filter content deemed illegal or offensive by that country.[90] This approach has three major advantages over the previous two methods.

First, it gives each country the ability to regulate speech according to its own standards without the need to enforce extraterritorial jurisdiction over foreign ISPs.[91] Filtering information at the national level allows governments to control what users view within their borders without concern for what ISPs post in other countries. Therefore, individuals can view information according to the speech laws of their respective country and online entities can publish without the fear of extraterritorial spillovers because each nation will only enforce its own laws rather than attempting to impose borders on Internet speech and commerce.

Second, filtering gives each country greater control over the enforcement of its laws.[92] Rather than issuing potentially unenforceable decisions, as in the *Yahoo!* case, countries could enforce their decisions by threatening to blacklist the offending foreign company.[93] The threatened company could then evaluate its economic interest within that country and decide whether or not to comply with that particular country's mandate.[94] Regardless of whether the ISP values access to that country and complies or decides to continue its regular activities and forego access, the government will remove the offensive and illegal information.

---

[90] *See* Fagin, *supra* note 13, at 451.

[91] *Id.*

[92] *See id.* at 451.

[93] *See id.* at 451–52.

[94] *See id.* at 452–53.

Third, private industry filtering does not significantly increase the cost of online publication. Rather than placing the economic burden of maintaining "a huge matrix of pages versus jurisdictions"[95] for each online content provider, local ISPs would be responsible for filtering according to its country's laws and could spread the expense among local subscribers.

Private industry filtering is a logical answer to online jurisdictional problems; however, certain negative effects may prevent implementation. First, the economic costs may be greater than originally thought. The threat of world-wide liability may cause global providers, such as America Online (AOL), to pull out of regions rather than comply with filtering requirements.[96] Second, many countries have laws that limit the liability of ISPs.[97] In these countries, courts do not perceive ISPs as content providers but as conduits for access to the Internet.[98] These countries would fear restricting access to the Internet if such a plan would impose financial and technical liability on local ISPs.[99]

One final negative effect of required filtering by ISPs is the potentially abusive power it lends to governments, opening the doors for repression of speech, as in China or Libya.[100] Critics fear that such an increase in governmental power to control content will create a society akin to that of George Orwell's 'Big

---

[95] *See* Laurie, *supra* note 24.

[96] Steve Kettmann, *Another Hate Site Trial in France*, WIRED NEWS, June 29, 2001, *at* http://www.wired.com/news/politics/0,1283,44908,00.html (last visited Apr.26, 2005).

[97] Fagin, *supra* note 13, at 453.

[98] *Id.*

[99] *Id.*

[100] Kerem Batir, *Regulating Hate Speech on the Internet: Unilateralism v Multilateralism, Technique v Law*, *at* http://inet-tr.org.tr/inetconf8/sunum/77.pdf (last visited Mar. 9, 2005).

Brother' novel.[101] This fear appears to stem from the past acts of speech-repressive governments, such as China, where authorities jail individuals for posting pro-democracy statements on the Internet,[102] or Iran where police arrested 70 schoolchildren for using the Internet to arrange dates.[103] Rather than trusting governments to refrain from abusing this power, critics of private industry filtering prefer alternative censorship methods.

Despite the criticisms outlined above, private industry filtering is the best of the three alternatives discussed in this article. Although some ISPs may choose to pull out of a region rather than comply with a country's monitoring and filtering laws, a private filtering regime can reduce these companies' concerns about high economic costs by limiting their liability through other legal means. ISP liability, for example, could be limited to allow only governmental agencies to take legal action against them for failure to make a reasonable and good faith effort to comply with filtering laws.[104] Although filtering compliance costs may be high for ISPs, the cost to content providers such as Yahoo! Inc. are similarly high. ISPs actually have the advantage over content providers because they have the ability to spread compliance costs among local subscribers; whereas content

---

[101] *Id.*

[102] *See* Reporters Without Borders, *The Internet Under Surveillance: Obstacles to the Free Flow of Information Online*, 31 (2003), *at* http://www.rsf.fr/IMG/pdf/doc-2236.pdf (last visited Mar. 9, 2003).

[103] *Id.* at 66.

[104] However, it should be understood that ISPs should not be required to achieve 100% filtration since that is not a current technological possibility. Lauric, *supra* note 24; *see* Andy McCue, *Yahoo Considers New World Order*, VNUNET.COM, Nov. 30, 2000, *at* http://www.vnunet.com/analysis/1114886 (last visited Apr.26, 2005). It is also important to remember that perfect filtration was not a requirement in *Yahoo!*. UEJF et LICRA v. Yahoo! Inc. et Yahoo France, T.G.I. Paris, May 22, 2000, N° RG: 00/05308, obs. C. Bensoam & J. Gomez, *translation available at* http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (last visited Apr. 26, 2005).

providers rely solely on advertising revenues which are dependent upon global access and breadth of content.[105]

The second negative effect discussed above, that many countries currently restrict ISP liability, may also have a solution if ISPs can filter illegal material while still complying with the applicable domestic legislation. The European Union Directive on Electronic Commerce provides an example of how this type of restriction may present a problem to private industry filtering: "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature."[106] On its face, the EU Directive appears to prohibit all blanket monitoring obligations, such as requiring local ISPs to filter all illegal material. However, the EU Directive does not affect specific monitoring cases: "orders by national authorities in accordance with national legislation," or the requirement that service providers exercise care in detecting and preventing illegal activities on services hosted by the provider.[107] It follows that ISPs could plausibly install filtering software and block specific sites made illegal through legislation as they come to the ISP's attention without violating the Directive. Thus, the WSIS presents an opportunity for the world to cooperate in amending the Directive and other countries' legislation to permit this type of filtering.

---

[105] *See* Le Menestrel, *supra* note 32, § 2.4. Analysts estimated that it would cost up to 25% of Yahoo! Inc.'s operating budget to comply with the French ruling. McCue, *supra* note 104.

[106] Parliament and Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce'), art. 47, 2000 O.J. (L 178) 1.

[107] *Id.* at art. 48.

The most popular criticism of regulating ISP filtering on a national level is the fear of oppressive censorship and undue governmental control, as explained above in reference to China and Iran.[108] Private industry filtering is, however, only superficially similar to such information control regimes. Mandated filtering by ISPs does not bestow new and extreme powers of control upon the government. France, for example, has already passed a statute making it illegal to sell or promote Nazi materials in France.[109] They have already enforced this statute in real world situations by banning the sale of *Mein Kampf* in online bookstores.[110] Requiring ISPs, rather than online entities, to filter the same content would extend regulation to the Internet without crossing the border into another nation's jurisdiction. Ultimately, as far as governmental objectives are concerned, there is little difference between mandating that Yahoo! Inc. filter Nazi articles from its site and mandating that French ISPs do the filtering. Indeed, requiring private industry filtering gives governments little censorship power beyond that which they already possess. It merely increases a country's ability to enforce its preexisting laws in this new and challenging medium. As illustrated in this article, many nations already attempt Internet content regulation.[111] Standardized private industry filtering will make such attempts more effective while avoiding many negative external spillover effects.

---

108 Fagin, *supra* note 13, at 451.

109 *See* UEJF et LICRA v. Yahoo! Inc. et Yahoo France, *supra* note 104 (finding Yahoo! Inc. in violation of article R. 645-2 of the penal code, which makes it illegal to display Nazi memorabilia).

110 *See* Le Menestrel, *supra* note 32, § 1.4.

111 *See generally* Reporters Without Borders, *supra* note 102.

Australia's recent implementation of a private industry filtering system illustrates the effectiveness of private industry filtering.[112] The goals of the Australian legislation include providing "a means for addressing complaints about certain Internet content; and to restrict access to certain Internet content that is likely to cause offence to a reasonable adult; and to protect children from exposure to Internet content that is unsuitable for children."[113] In order to accomplish these goals, the legislation gives the Australian Broadcasting Association (ABA) authority to investigate the availability of prohibited or potentially prohibited content and allows the ABA to investigate content complaints.[114] If, after the investigation, the ABA determines that the content falls within one of the prohibited classifications, its next decision depends on whether the content is hosted in Australia or not. If the content is hosted on Internet severs in Australia, the ABA issues a final notice directing the host to discontinue hosting the offensive content.[115] If the content is hosted on a server site outside of Australia, the ABA mandates the ISP to follow industry codes or content filtering standards.[116]

As compliance with ABA industry filtering standards is mandatory,[117] the burden of censoring content rests solely on the service provider or content host,

---

[112] Broadcasting Services Amendment (Online Services) Act, 1999, sched. 1 (Austl.), *available at* http://www.users.bigpond.com/baker5153/amended.html (last visited May 4, 2005) (now included as sched. 5 of the Broadcasting Services Act, 1992 (Austl.), *available at* http://www.aba.gov.au/legislation/bsa/ (last visited Mar. 9, 2005)).

[113] Broadcasting Services Amendment (Online Services) Act, 1999, *supra* note 112, at 1.

[114] *Id.* at Part 1, §§ 26(1), 27(1).

[115] *Id.* at Part 1, § 2.

[116] *Id.*

[117] *Id.* at Part 5, § 52.

leaving no obligation on the producers of content or those who access or upload content.[118] If an ISP or content host fails to comply, the ABA may issue a formal warning and apply to the Federal Court for a compliance order.[119] Compliant ISPs and hosts are free from civil liability for blocking content.[120] Regulatory strengths or weaknesses do not lie in the straightforward process set forth in the legislation, but in the industry filtering codes and standards.

The Internet Industry Association (IIA) drafted the ABA's current code.[121] In drafting the code, the IIA attempted to balance industry interests with the government's interest in blocking offensive material.[122] The code established by the IIA "does not impose *any* requirement for ISPs to engage in universal blocking of content which the ABA deems prohibited."[123] It only "requires that ISPs provide certain classes of end users with tools by which means they can control the access of content into the home,"[124] effectively placing content control in the end users' hands. Additionally, there is no requirement that the end user actually use the filtering product provided by the ISP.[125] The code also furnishes ISPs with approved filters to satisfy the requirement of providing tools to the end user.[126] In 2000, the list of approved filters rose to sixteen with over

---

[118] *Id.* at Part 1, § 1(2).

[119] *Id.* at Part 6, §§ 84-85.

[120] *Id.* at Part 8, §§ 88.

[121] Carolyn Penfold, *The Online Services Amendment, Internet Content Filters, and User Empowerment*, 7 N.L.R. §§ 8-9 (2000), *available at* http://pandora.nla.gov.au/parchive/2001/Z2001-Mar-3/web.nlr.com.au/nlr/HTML/Articles/penfold2/penfold2.htm (last visited Mar. 9, 2005).

[122] *Id.* § 9.

[123] Industry Internet Association, *IIA Content Regulation Code of Practice (version 7.2),available at* http://www.iia.net.au/contentcode.html (last visited Mar. 9, 2005).

[124] *Id.*

[125] Penfold, *supra* note 121, § 10.

[126] *Id.*

one hundred more available on the market.[127] Although the study and criteria used to assess the filters placed on the list failed to evaluate the actual effectiveness of the different filters,[128] the market is likely to produce more effective filtering products than those currently approved by the ABA.[129]

Based on the Australian legislation's original goal to restrict access to offensive content, the law appears ineffective because it lacks a mandatory filtering requirement for ISPs and the approved filters may possibly be less effective than the commercially available filters. However, the IIA's "industry facilitated user empowerment"[130] approach leaves the ultimate choice of censorship in the hands of the user rather than the government. Other countries may consider adopting this approach because it alleviates reservations regarding grants of governmental censorship power.

D. Content Labeling

Private industry filtering will be far more effective if implemented in combination with the Platform for Internet Content Selection (PICS)[131] and a standardized content labeling vocabulary such as the one developed by the Internet Content Rating Association (ICRA). PICS provides a standard convention for digital label formats and distribution methods without actually

---

[127] *Id.* § 51.

[128] *Id.* § 15.

[129] *Id.* § 51.

[130] Industry Internet Association, *supra* note 123.

[131] For more details regarding PICS, visit http://www.w3.org/PICS/ (last visited Mar. 5, 2005).

creating labels or labeling Internet content itself.[132] It merely provides a way for all PICS-compliant filtering software to read the labels regardless of what program generated the label. The ICRA works in harmony with the PICS by providing an internationally accepted voluntary rating system using PICS labels.[133] The ICRA does not rate sites, but rather provides a system for content creators to label their site with "an objective, descriptive label."[134]

The PICS system has the advantage of allowing each nation to determine via PICS labels and national law which sites ISPs must filter, all without affecting other nations' access to the material or restraining online speech and commerce. Additionally, the labels themselves are neutral and merely describe what the site contains. Unfortunately, few content creators apply labels on a voluntary basis, leaving many sites unlabeled and rendering national filtering schemes ineffective. The WGIG found that in practice, the ICRA software failed due to the lack of a "critical mass of sites labeling their content."[135]

The ICRA and other label filtering software can be effective if world governments unify and agree upon labeling methods; and provide incentives for content creators to label their sites. For example, governments could eliminate content creator's liability in foreign jurisdictions if they have properly labeled

---

[132] Paul Resnick & James Miller, *PICS: Internet Access Controls Without Censorship*, 39(10) COMMUNICATIONS OF THE ACM 87 (1996), *available at* http://www.w3.org/PICS/iacwcv2.htm (last visited Mar. 17, 2005). All content and information on the Internet can be "labeled" or identified in the broadcast stream to "reflect diverse viewpoints" and allow software to block content with specific labels. *Id.* The PICS is "analogous to specifying where on a package a label should appear, and in what font it should be printed, without specifying what it should say." *Id.*

[133] Internet Content Rating Association, *Answers to FAQs about ICRA*, FAQs 1.1, 4.1, *at* http://www.icra.org/faq/abouticra/ (last visited Mar. 17, 2005).

[134] *Id.* at FAQ 4.2.

[135] Working Group on Internet Governance, *Issue Paper*, *supra* note 1, § 8.

their sites. If content creators fail to properly label their site, they would be subject to suit in any jurisdiction that has access to the information, as in an effects-based jurisdiction analysis. Another alternative that would help create the necessary critical mass of labeled sites is requiring proper labels prior to domain name registration. Private industry filtering, therefore, avoids the external costs of an effects-based analysis and can give each government greater control over unlawful sites.

IV. CONCLUSION

The WGIG recognizes that "[l]eaving things as they are creates uncertainty on the part of content providers."[136] "[S]ome kind of best practice" is needed at the very least.[137] Each of the three methods discussed above have advantages and disadvantages. Of the three, private industry filtering combined with standardized content labeling provides the best alternative, enabling nations to enforce their laws on the Internet without extending the effects of those laws into other nations. Accordingly, the WGIG and WSIS would be wise to adopt the "best practice" of private industry filtering to deal with the uncertainty of extraterritorial Internet jurisdiction.

Jay Wahlquist

[136] *Id.* § 3.
[137] *Id.*