UIC John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 1 *Journal of Computer & Information Law - Fall 2004*
Article 3

Fall 2004

Geo-Location Technologies and Other Means of Placing Borders on the 'Borderless' Internet, 23 J. Marshall J. Computer & Info. L. 101 (2004)

Dan Jerker B. Svantenson

GEO-LOCATION TECHNOLOGIES AND OTHER MEANS OF PLACING BORDERS ON THE 'BORDERLESS' INTERNET

DAN JERKER B. SVANTESSON†

Until recently, it was frequently said to be impossible or at least pointless to attach significance to 'location' in the online arena.[1] Indeed, the impossibility of linking those active on the Internet, to a geographical location was seen as a distinctive feature of the Internet. However, this is all changing. A recent survey revealed that a large number of companies, particularly in the U.S., seek to identify the geographical location of those who visit the companies' Web sites.[2] While it is still true that Internet communication largely lacks reliable geographical identifiers, several non-technical methods are applied to cater for the need to know the location of those active on the Internet. Furthermore, so-called geo-location technologies are becoming increasingly accurate, and while unlikely to ever be one hundred percent accurate, may, in the near future or

† Assistant Professor, Faculty of Law Bond University, Gold Coast Queensland 4229 Australia, Ph: +61 7 5595 1418, E-mail: Dan_Svantesson@bond.edu.au, (www.svantesson.org) - Research Associate, Baker & McKenzie Cyberspace Law and Policy Centre - Contributing Editor, World Legal Information Institute (www.worldlii.org) - National Convener, International Law Interest Group (Australasian Law Teachers Association) - National Rapportuer (Australia) Data Protection Research and Policy Group, British Institute of International and Comparative Law.

1. *See e.g.* David Johnson and David Post, *Law And Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996); *see also American Libraries Association v Pataki* (969 F.Supp. 160, 170 (S.D.N.Y. 1997); *see also* more recent works such as: Henrik Spang-Hanssen, *Cyberspace Jurisdiction in the U.S. – The International Dimension of Due Process* 3 (2001).

2. Michael Geist, *et al.*, *Global Internet Jurisdiction: The ABA/ICC Survey* (April 2004), http://www.mgblog.com/resc/Global%20Internet%20Survey.pdf (accessed May 25, 2004)

> Thirty-seven percent of responding companies indicated that they seek to identify user location, while thirty eight percent responded that they did not, and twenty percent of respondents were unsure, perhaps reflecting a lack of communication between technical Web site administrators (who manage and implement user identification solutions) and legal counsel (who constituted the majority of survey respondents).

perhaps already today, be accurate enough for legal purposes. Yet the questions that these developments give rise to have gained surprisingly little attention in literature. Against this background, the article examines the different ways in which a Web site operator can identify the geographical location of those accessing its Web site, and the legal implications of such identification.

While a range of purposes, such as fraud detection, authentication, content targeting, security and network efficiency has been envisaged for geo-identification in general, and geo-location technologies in particular,[3] it is primarily the use of geo-location technologies for conditioning access and legal compliance that is of concern for this article.

Finally by way of introduction, for the purpose of an overview such as the one provided in this article, it is useful to draw a number of distinctions. First, it should be acknowledged that geo-location technologies are not the only ways in which a Web site operator may seek to identify the geographical location of the access-seeker. I therefore distinguish between *hard protection* provided by geo-location technologies and the *soft protection* provided by alternative non-technical means. Secondly, since the level of complexity of different geo-location technologies varies greatly, I draw a distinction between *sophisticated geo-location technologies* and *unsophisticated geo-location technologies*. Before these different categories are discussed in detail, a few more words should, however, be said about the context in which geo-identification is relevant.

I. THE CONTEXT

If a Web site operator can know the location of those who access the Web site, he/she can, due to the reactive nature[4] of Web servers, control what material is presented, and indeed, accessible to each access-seeker. In addition to business advantages, such as targeted advertisement, a structure allowing for geo-identification has the advantage of providing the Web site operator with the means to comply with local regulations. Indeed, as the provided content can be adjusted depending on the access-seekers' geographical location, geo-identification has the advantage of

3. *See e.g. Internet Geography Guide – A NetGeo White Paper* (can be requested from http://www.netgeo.com/ (accessed May 25, 2004)).

4. A Web server's function is most accurately described as *reactive*. The content of a Web site is not constantly broadcasted, or even available in any humanly comprehensible format, but at the moment the server receives an access-request, the content becomes available – the server reacts to the browser's request/action. Describing the web servers' role as reactive is, further, preferable as it indicates active steps of both the one imparting the information and the one receiving the information (i.e. the receiver acts and the sender reacts); *see* Roger Clarke, *Defamation on the Web: Gutnick v. Dow Jones*, http://www.anu.edu.au/people/Roger.Clarke/II/Gutnick.html (accessed May 25, 2004) (explaining the term reactive).

providing the Web site operator with the means to comply with multiple, varying, and even contradictory, local regulations. The value of this cannot be emphasised enough in a world where substantive laws vary considerably from state to state, but materials may be accessible from every state where Internet connection is possible. The need for Web site operators to take active steps to regulate their legal exposure is obvious when the current rules of conflict of laws, or private international law as the field is referred to in civil law countries, are considered. As is exemplified by the High Court of Australia's judgment in *Dow Jones & Company Inc. v. Gutnick*[5], many states will, for example, exercise jurisdiction over, and apply its laws to, a foreign publisher if the defamatory material published by that publisher entered the mind of somebody within that state. Similar reasoning, in the online context, can, for example, be found in the British *Harrods* case,[6] the Canadian *Bangoura* case,[7] and the *Investasia* case[8] from Hong Kong SAR. Furthermore, the need for Web site operators to take active steps to regulate their legal exposure has been acknowledged in the context of the development of a new international convention. Article 7 of the previously proposed *Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters* stated that: "activity shall not be regarded as being directed to a State if the other party demonstrates that it took *reasonable steps* to avoid concluding contracts with consumers habitually resident in the State."[9] This sort of regulatory approach clearly illustrates the necessity of Web site operators actively limiting their legal exposure. As far as the U.S. rules of jurisdiction are concerned, we can suitably focus on the test established through *International Shoe Co. v. Washington*:[10]

> [D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain *minimum contacts* with it such that the maintenance of the suit does not offend *'traditional notions of fair play and substantial justice'*.[11] (emphasis added)

A Web site operator with the ability to determine the geographical location of those who access his/her Web site would be in a good position

5. *Dow Jones & Company Inc v. Gutnick* [2002] HCA 56.

6. *Harrods Ltd. v. Dow Jones & Company Inc.* [2003] EWHC 1162 (QB).

7. *Bangoura v. Washington Post* (Jan. 27, 2004) OSCJ 03-CV-247461CM1.

8. *Investasia Ltd and Another v. Kodansha Co Ltd and Another* HKCFI 499 (18 May 1999).

9. *See* Article 7, *Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters* (June 2001 Draft) (emphasis added) (Article 7 existed in several different forms, and the quoted text was not by any means uncontroversial. Further, presently it seems unlikely that the convention proposal will become a reality. However, it is nevertheless important to note that this sort of reasoning is present).

10. *International Shoe Co. v. Washington*, 326 U.S. 310 (1945).

11. *Id.* at 316.

to avoid *minimum contact* being established between him/her and undesirable locations. To examine this further, it is useful to draw upon the facts of a couple of Internet related court cases. One of the leading cases, as far as U.S. Internet defamation is concerned, is *Young v. New Haven Advocate*.[12] There two newspapers based outside Virginia published articles, in part discussing the conduct of residents of Virginia, in Virginia.[13] The articles were available both offline and online. Despite this, the United States Court of Appeals for the Fourth Circuit concluded that:

> The newspapers did not post materials on the Internet with the manifest intent of targeting Virginia readers. Accordingly, the newspapers could not have "reasonably anticipated being haled into court [in Virginia] to answer for the truth of the statements made in their articles." *Calder*, 465 U.S. at 790 (quotation omitted). In sum, the newspapers do not have sufficient Internet contacts with Virginia to permit the district court to exercise specific jurisdiction over them.[14]

Throughout the judgment, the Court made frequent reference to a copyright case decided a couple of months earlier. In *ALS Scan, Inc. v. Digital Service Consultants, Inc.*[15].the Court formulated the following test, based on the *Zippo* test:[16]

---

12. *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir. 2002).

13. Maximum-security prisons in Connecticut were overcrowded, and as a consequence, Connecticut had contracted with Virginia to house a number of Connecticut prisoners. The articles, in question, discussed the state of a penal institution in Virginia as well as the conduct of its warden.

14. *Young* at 315 F.3d 256 at 265; *see e.g.*, Gregory J. Wrenn, *Cyberspace is Real, National Borders are Fiction: The Protection of Expressive Rights Online Through Recognition of National Borders in Cyberspace*, 38 Stan. J. Int'l. 97 (2002) (the targeting approach has also been strongly advocated in a recent literature).

15. *ALS Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Cir. 2002).

16. *Zippo Manufacturing Company v. Zippo Dot Com, Inc.* 952 F.Supp. 1119 (W.D.Pa. 1997) (In the context of jurisdiction over online activities, this case must be seen as somewhat of a landmark case.) By drawing a distinction between different types of Web sites and by dividing Internet presence into three separate categories, the Court established a 'sliding scale' test:

> [O]ur review of the available cases and materials reveals that the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is deter-

> [W]e conclude that a State may, consistent with due process, exercise judicial power over a person outside of the State when that person (1) directs electronic activity into the State, (2) with the manifested intent of engaging in business or other interactions within the State, and (3) that activity creates, in a person within the State, a potential cause of action cognizable in the State's courts. Under this standard, a person who simply places information on the Internet does not subject himself to jurisdiction in each State into which the electronic signal is transmitted and received. Such passive Internet activity does not generally include directing electronic activity into the State with the manifested intent of engaging business or other interactions in the State thus creating in a person within the State a potential cause of action cognizable in courts located in the State.[17]

By considering part one and part two of the test together, the Court in *Young v. New Haven Advocate* modified the *ALS Scan* test to work "more smoothly" for cases where the Internet activity is the posting of news articles on a Web site:[18] "We thus ask whether the newspapers manifested an intent to direct their Web site content – which included certain articles discussing conditions in a Virginia prison—[sic] to a Virginia audience."[19] While the defendant was successful in this particular case, it would have been better if the publishers had employed means to limit the online distribution of their publications to those states in which they would be prepared to defend a dispute relating to the publications. In more detail, if a publisher is aware that it is publishing material that may defame a person residing in another state, the publisher would be well-advised to seek to avoid publishing the material in that state. The defendants in *United States v. Thomas*[20] was not as fortunate as the defendants in *Young v. New Haven Advocate*. In *Thomas*, the defendants had made pornographic material available over the Internet to subscribers located in various U.S. states. Following up a complaint, a United States Postal Inspector used an assumed name and became a subscriber of the defendants' service as part of an undercover operation. After the Postal Inspector had downloaded sexually explicit images, the defendants were charged. In that particular case, the defendants knew the subscribers' addresses and could thus easily have chosen to limit their legal exposure. However, if the defendants would have provided their material on an open-and-free-for-all Web site, where the access-seekers are not required to provide any information, knowing which states' laws and ju-

---

mined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

Id.

17. *ALS Scan, Inc. v. Digital Service Consultants, Inc.*, 293 F.3d 707 (4th Cir. 2002).

18. *Young v. New Haven Advocate*, 315 F. 3d 256 (4th Cir. 2002).

19. *Id.*

20. *United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996).

risdictions the Web site operators were exposing themselves would have been more complicated. It is submitted that, in any situation where a Web site operator is providing content that is legal in the state where he/she is located, but illegal in other states, it would be highly beneficial for the Web site operator to be able to identify the access-seekers' physical location.

In light of the above, it is clear that, as long as states apply conflict of laws rules that focus on the location of the effect rather than on the location where the defendant acted, there is a need for Web site operators to take steps to limit the geographical spread of their content. If we also consider the fact that courts, as discussed below, increasingly are taking notice of the possibilities of geo-identification, the conclusion must necessarily be that Web site operators are well-advised to review their online business models, and should consider the use of geo-identification.

II. HARD PROTECTION – TECHNICAL MEANS OF GEOGRAPHICAL IDENTIFICATION

Lawrence Lessig brought popular attention to, and increased understanding of, the fact that the Internet is being regulated both through law and technical developments in his widely read *Code and Other Laws of Cyberspace*.[21] One of his main points is neatly summarised in one of his earlier articles:

> I said that we could understand regulation in real space as a function of four sorts of constraints-law, norms, markets, and what I called real space code [also referred to as architecture[22]]. We can understand regulation in cyberspace in the same way. Regulation in cyberspace is a function of similar constraints. It too is a function of the constraints of law, of norms, of the market, and of what I will call, 'code.'[23]

Lessig also noted that "[t]he constraints are distinct. Yet they are plainly interdependent."[24] In other words, laws affect the market, the norms and the code/architecture (and thereby provide indirect regulation). But at the same time, the creation of laws takes account of the market, of the norms and the code/architecture. Changes in the market situation may spark the creation of new laws,[25] a change in norms may

---

21. Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

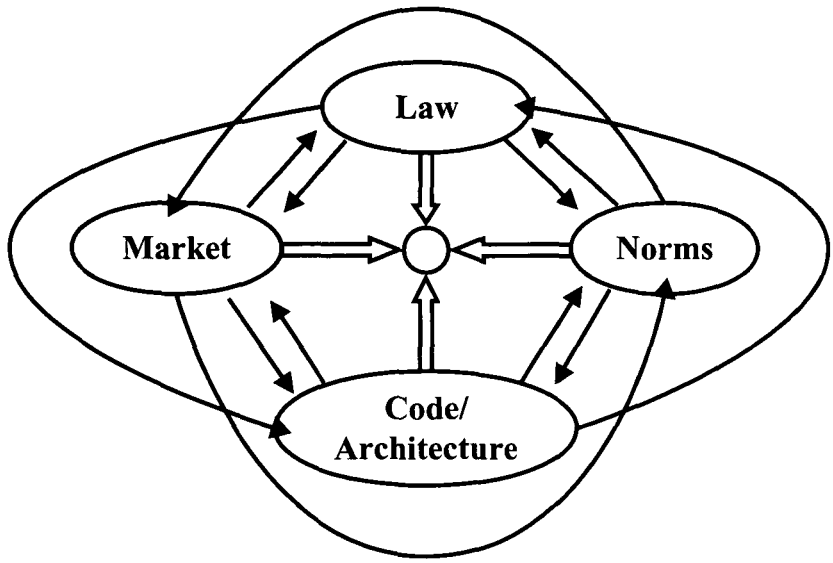
22. *Id.*

23. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, Stan.Tech. L. Rev. (1997) (no longer available online); *see further* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 506-508 (1999).

24. Lawrence Lessig, *Code and Other Laws of Cyberspace*, 88 (Basic Books).

25. *E.g.*, legislation against competition restrictions or as it also is called anti-trust.

lead to a change in laws,[26]and the development of code/architecture affects the law.[27] In addition, norms affect the market and code/architecture, code/architecture affects the market and norms, and the market affects code/architecture and norms – all these four regulatory mechanisms clearly affect each other.[28] Thus, the following figure, in which the circle in the centre represents the object being regulated, can be used to illustrate regulation:



⟹ Direct regulation

→ One regulatory mechanism's effect on another, leading to an indirect effect on the area being regulated.

An awareness of the interaction between these regulatory mechanisms is essential when evaluating the influence of geo-location technologies as part of code/architecture. It is, therefore, necessary to look in more detail at how the three other regulatory mechanisms (i.e. norms, market and laws) affect, and are affected by, the regulatory influence of geo-location technologies.

As far as geo-location technologies are concerned, it is plain to see that norms may affect its use, but currently, it is difficult to know whether norms will strengthen or weaken the regulatory influence of

26. *E.g.*, As the general public's view of marriage has changed; de facto relations have, at least to an extent, been given the same status as marriages.

27. For a discussion of the French court's reference to geo-location technologies in the *Yahoo!* case, see discussion below.

28. Not necessarily to an equal extent, however.

geo-location technologies. Society has not yet been sufficiently exposed to geo-location technologies for there to be any norms in relation to their use, and if anything, it could perhaps be assumed that a number of users will react negatively to discrimination based on location. For the same reasons, it is also difficult to predict how, if at all, geo-location technologies may affect norms.

In contrast, it is obvious that the market has started to embrace the use of geo-location technologies, which has a strengthening effect on the regulatory influence of geo-location technologies. Turning to the influence that geo-location technologies may have on the market, it would seem likely that these technologies will give the market greater control (e.g. different prices in different countries) and thereby enhance the market's regulatory powers.

The fact that lawmakers take account of technological developments (i.e. code/architecture) is of central importance when examining the potential uses of geo-location technologies – in properly understanding the significance of geo-location technologies, one must realise that changes in technology may spark changes in law, or the application of law. In this context, it is interesting to note the difference in approach between the landmark 1997 U.S. decision in *Reno v. ACLU.* [29] and the Australian Internet defamation case, *Macquarie Bank Limited & Anor v. Berg*,[30]on the one hand, and the French Court's 2000 decision in *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.*[31] on the other. In *Reno v. ACLU*, Justice O'Connor stated that "[u]ntil gateway technology is available throughout cyberspace, and it is not in 1997, a speaker cannot be reasonably assured that the speech he displays will reach only adults because it is impossible to confine speech to an 'adult zone.'"[32]– the lack of feasible technical solutions was determinative in the case. In *Macquarie Bank Limited & Anor v. Berg*, the plaintiffs were seeking an injunction restraining the defendant from publishing allegedly defamatory material on a particular Web site, and Simpson J stated that:

> The limitation [to publication occurring in NSW only] is ineffective. Senior council [for the plaintiffs] acknowledged that he was aware of no means by which material, once published on the Internet, could be excluded from transmission to or receipt in any geographical area. Once published on the Internet material can be received anywhere, and it

29. *Reno v. ACLU,* 521 U.S. 844 (1997).

30. *Macquarie Bank Limited & Anor v. Berg* [1999] NSWSC 526.

31. *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.* County Court of Paris, interim court order of 20th of November 2000 (English translation available at http://www.cdt.org/speech/international/001120yahoofrance.pdf (accessed May 25, 2005).

32. *Reno v. ACLU,* 521 U.S. 844, 891 (1997) (O'Connor, J., dissenting).

> does not lie within the competence of the publisher to restrict the reach of the publication.[33]

There can be no doubt that the technical features of the Internet played a central role in the judge's decision not to give injunctive relief in *Macquarie Bank Limited & Anor v. Berg*. In contrast, based on the expert evidence provided, Justice Gomez in the *Yahoo!* case, concluded that geo-location technologies are sufficiently effective to allow the defendant to implement them to prevent access-seekers located in France from accessing the Nazi memorabilia/junk in dispute.[34] Here, the perceived existence of feasible technical solutions was determinative. In conclusion, code, or architecture, certainly provide indirect regulation through law. Furthermore, the fact that courts have started to take account of geo-location technologies is a huge incentive for continued development. This, in turn, is likely to lead to improved accuracy, and this improved accuracy can motivate courts to place an even heavier emphasis on these technologies.

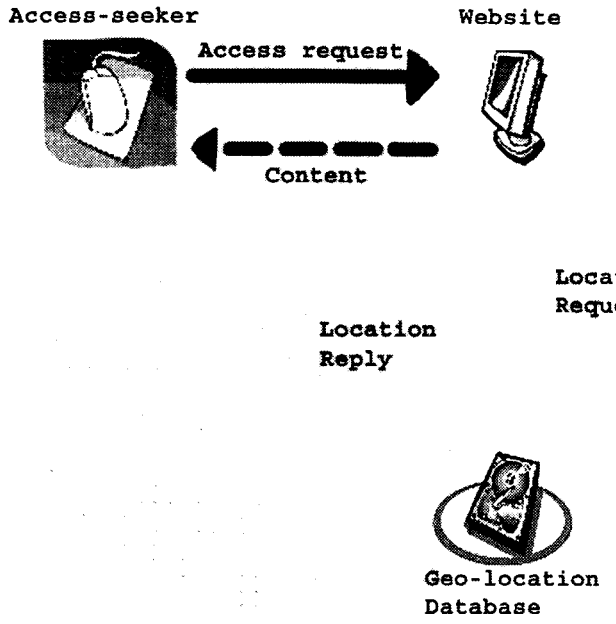
A. Sophisticated Geo-location Technologies

Currently the only form of geo-location technology that can be called sophisticated is geo-location technologies that use the translation of IP addresses[35] into geographical locations, based on information stored by the provider of the geo-location service. The figure below illustrates a common model of how this form of geo-location technology is applied:

33. *Macquarie Bank Limited & Anor v. Berg* [1999] NSWSC 526, at para 12.

34. *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.* County Court of Paris, interim court order of 20th of November 2000 (English translation available at http://www.cdt.org/speech/international/001120yahoofrance.pdf (accessed May 25, 2004)).

35. *See above*. There is currently approximately 1.3 – 1.6 billion IP addresses in use, out of the 4.25 billion possible addresses that can be issued under the four block range from 0 to 255. (*See further*: Alex van Leeuwen, *Geo-targeting on IP Address: Pinpointing Geolocation of Internet Users*, Geo Informatics (July/Aug. 2001); *see also* Stefanie Olsen, *Geographic Tracking Raises Opportunities, Fears,* http://news.com.com/Geographic™racking® aises+opportunities%2Cêars/2100-1023_3248274.html (accessed Nov. 8, 2000); and Todd Spangler, *They Know – Roughly – Where You Live*, eWEEK, Aug. 20, 2001.



As the access-seeker enters the appropriate Uniform Resource Locator ("URL")[36] into his/her browser, or clicks on the appropriate hyperlink, an access-request is sent to the server operating the requested Web site. As the server receives the access-request, it, in turn, sends a location request (e.g. forwards the access-seeker's Internet Protocol ("IP") address)[37] to the provider of the geo-location service. The provider of the geo-location service has gathered information about the IP addresses in use, and built up a database of geo-location information.[38] Based on the information in this database, the provider of the geo-location service gives the Web site server an educated guess as to the access-seeker's location. Armed with this information, the Web server can provide the access-seeker with the information deemed suitable (e.g. a message along the lines of: "Sorry. This Web site is intended for the people of Sweden

36. Webopedia, *URL*, http://www.webopedia.com/TERM/U/URL.html (accessed May 25, 2004)

("[URL], Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.");

see e.g., Laura A. Chappell and Ed Tittel, Guide to TCP/IP 271 (2002).

37. *See* SearchWebServices.com, *IP Address,* http://searchwebservices.techtarget.com/sDefinition/0,sid26?gci212381,00.html (accessed May 25, 2004).

38. The methods of collecting this information are discussed below.

only,"[39] or perhaps provide advertisement specifically targeted at people from the access-seeker's particular location). There are currently several products on the market utilising this type of system.[40] This technology is not necessarily prohibitively expensive for larger Web site operators, nor does it appear particularly difficult to operate.[41]

1. *Accuracy*

The accuracy of these products is difficult to gauge. While the providers indicate the potential accuracy to be very high, it should be remembered that they, after all, are trying to sell a product and thus arguably could be forgiven for presenting their technology in the best light possible. For example: "Akamai says it can accurately identify a North American user's city at least 85% of the time, while NetGeo promises an 80% success rate for cities worldwide;"[42] Digital Envoy claims that their product "NetAcuity covers 99.9% of the Internet, and provides accuracy rates of over 99% at a country level and approximately 92% at a city-level worldwide;"[43] and, while presumably discussing the technology in general terms, Alex van Leeuwen[44] states that "[t]he present accuracy is about 97.5% on country recognition."[45] In relation to all these impressive figures, it has been said that:

39. Showtime, *Homepage*, http://www.sho.com, (accessed May 25, 2004) (for an example, when using a computer at University of New South Wales (Australia), to access Showtime's Web site, I received the following message: "We at Showtime Online express our apologies; however, these pages are intended for access only from within the United States.").

40. *See e.g.* Quova, *Homepage,* http://quova.com (accessed May 25, 2004); Akami, *Homepage*, http://www.akamai.com (accessed May 25, 2004); Caida, *NetGeo – The Internet Geographic Database,* http://www.caida.org/tools/utilities/netgeo (accessed May 25, 2004); Digital Envoy, *Homepage*, http://www.digitalenvoy.net/ (accessed May 25, 2004); Perl-studio, *IP-ISP Country Database in PHP,* http://www.perl-studio.com/ipcountry/index.php. (accessed May 25, 2004); Active Target, *Live Demo*, http//:www.activetarget.com/livedemo.asp (accessed May 25, 2004); IP2Location, *Homepage*, http://www.ip2location.com/free.asp (accessed May 25, 2004); and Geobytes, *IP Address Locator*, http://www.geobytes.com/IpLocator.htm (accessed May 25, 2004).

41. The author does not have sufficient information, and is anyhow not qualified, to independently assess the accuracy of these products. *But see* Geobytes, *Homepage*, http://www.geobytes.com (accessed May 25, 2004) (for an example, Geobytes' product is available from $500 U.S. per annum and appears easy to operate); *see also* Geobytes, *Demo*, http://www.geobytes.com (accessed May 25, 2004) (where producers argue that the product is accurate to 97 percent on country-level and 75-80 percent on city-level).

42. Todd Spangler, *They Know – Roughly – Where You Live*, eWEEK, (Aug. 20, 2001).

43. Digital Envoy product sheet (on file with the author).

44. Judging from his e-mail address, an employee of Quova (a manufacturer of geolocation products).

45. Alex van Leeuwen, *Geo-targeting on IP Address: Pinpointing Geolocation of Internet Users*, Geo Informatics (July/Aug. 2001).

> The way the vendors arrive at their accuracy statistics is to cross-check the physical location of sampling of Internet users (as determined by their software) against customer provided locational information already in the possession of the software vendors. There is no way to independently verify whether the software could provide the claimed levels of accuracy if the software vendors didn't first have other customer location information which their software may be using to determine customer location. Put somewhat differently, it is as if a "psychic" claimed to be able to accurately know what card a customer held in their hand 99.5% of the time, and to prove it, the psychic would ask to see the cards in the hands of a sampling of customers before announcing that indeed those were the same cards he knew the customers to possess.[46]

In the French Court's judgment in the *Yahoo!* case, experts stated that "it may be estimated in practice that over 70% of the IP addresses of surfers residing in French territory can be identified as being French."[47] However, it is vital to bear in mind that the accuracy of these technologies is dependent on several factors and the accuracy-rate identified by the French Court is specific to the French context. Similarly, as pointed out by Benjamin Edelman:

> If a company were to assert that its method is, for example, '98% accurate' on average across all its applications involving analysis of locations throughout the world, it is likely that the accuracy rate for Canadian and American location distinctions alone is lower than 98%, given the unique difficulties in this context.[48]

With this in mind, it is important for other courts to take the same approach as the French Court in the *Yahoo!* case did, and be specific about the context of concern. The courts must avoid placing the focus on the marketing-driven *average* accuracy-rates presented by the companies behind the geo-location technologies, and instead pay attention to

---

46. Information Technology Association of America, *ECommerce Taxation and the Limitations of Geolocation Tools* 6, http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf (accessed May 25, 2004).

47. *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.* County Court of Paris, interim court order of 20th of November 2000 (English translation available *at* http://www.cdt.org/speech/international/001120yahoofrance.pdf (accessed May 25, 2004)). However, it would seem that one of the experts, Ben Laurie, later felt a need to explain his statement. (Ben Laurie, *An Expert's Apology*, *at* http://www.apache-ssl.org/apology.html (accessed May 25, 2004)).

48. Benjamin Edelman, *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users*, 6, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (accessed May 25, 2004) (The "unique difficulties" Mr Edelman speaks of are multiple). First, a number of ISPs offer their services in both U.S. and Canada. *Id.* Second, the proximity and economic ties between the two countries means that many companies have offices in both countries. *Id.* Third, the widespread use of intranets with a single access point to the Internet. *Id.* Fourth, communication between Canada and the U.S. is not particularly likely to pass through well-known "peering points" or contain the telltale transoceanic time delays. *Id.*

the *context-specific* accuracy rate. While this approach is likely to require expert witnesses in each individual case, at least on an initial level, and thereby be costly, it ensures that the courts base their decisions on the accuracy rate that is relevant in the particular case at hand.

There is a range of factors affecting the accuracy of geo-location technologies. Due to the dual nature of the geo-location process, these factors can be divided into two categories: 'source problems' and 'circumvention problems.'

The source problems are the problems associated with building up and/or collecting accurate geo-location data. In relation to IP addresses, there is no real equivalent to the address registers listing physical addresses, or the phone registers listing phone numbers, at least not currently. Consequently, the ones creating databases of geo-location information must rely on other, less straightforward, methods. Obviously, the accuracy of the material in the geo-location databases depend on, and can never be better than, the accuracy of the collection of that data. Thus, the collection of background material is vital. Common methods of collecting relevant material include, for example, gathering data from registration databases,[49] network routing information, DNS systems, host name translations, ISP information and Web content.[50] As discussed in detail by Edelman, all of these sources may provide inaccurate information.[51]

The second category, circumvention problems, is probably pretty self-explanatory – there are several methods for people with sufficient motivation[52] and knowledge to circumvent geo-location technologies. While some circumvention techniques are technologically advanced (e.g. deep linking to streaming video content without accessing the HTTP

49. Reseaux IP Europeens Network Coordination Centre, Homepage, http://www.ripe.net (accessed May 25, 2004). American Registry for Internet Number, Homepage, http://www.arin.net (accessed May 25, 2004). Asia Pacific Network Information Centre, Homepage, http://www.apnic.net (accessed May 25, 2004). Latin American and Caribbean IP Address Regional Registry, Homepage, http://lacnic.net (accessed May 25, 2004).

50. *See e.g.* Netgeo, *Internet Geography Guide – A NetGeo White Paper,* http://www.netgeo.com (accessed May 25, 2004).

51. Benjamin Edelman, *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users,* 3-7, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (accessed May 25, 2004).

52. As correctly noted by Edelman, the motivation for circumventing geo-location technologies seems to vary in accordance with the value of the content and while few people would feel any need to try to circumvent geo-location technologies aimed at providing location-specific advertisement, people would have a much greater incentive to circumvent geo-location technologies aimed at, for example, keeping non-residents of a particular forum from gaining access to free online TV broadcasts.; *see* Benjamin Edelman, *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users,* 7, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (accessed May 25, 2004).

server),[53] others are easy enough to be used by virtually anyone (e.g. anonymising techniques)[54] or even inherent in the system-structure ("tunnelling methods").[55] With this in mind, it will presumably always be possible to circumvent geo-location technologies. Having said that, it should also be noted that for most uses, these technologies do not need to be hundred percent accurate and it consequently does not always matter that they can be circumvented by a limited group of people motivated to do so. As stated by Goldsmith/Sykes:

> [M]any will point to the imperfections and conclude that the technologies "won't work" or are "infeasible" or "useless." This is a persistent error in thinking about Internet regulation; the conclusion simply does not follow from the premise. Regulatory slippage is a fact of life in real space and cyberspace alike. We do not conclude from the fact that minors obtain and use fake identification to purchase beer, or that thieves sometimes crack safes, or that gray market goods are imported into the United States, that drinking laws and criminal laws and trademark laws are useless. Nor should we assume that imperfections in Internet identification and filtering technology render these technologies useless. Regulation works by raising the cost of the proscribed activity, and not necessarily by eliminating it. Computer savvy users might always be able to circumvent identification technology, just as burglars can circumvent alarm systems. But they do so at a certain cost, and this cost is prohibitive for most.[56] (footnotes omitted)

While, as noted initially in this section of the article, the accuracy of the geo-location technologies is difficult to gauge, and is affected by both source problems and circumvention problems, at least one important conclusion can be drawn – the accuracy is high enough to interest Web site operators in using geo-location technologies, and high enough for the courts to start taking notice of geo-location technologies.

2. *False Positives and/or False Negatives*

As noted by Roger Clarke, one effect of the technologies not being one hundred percent accurate is the occurrence of false positives and/or false negatives.[57] That is: people that should not be allowed access will get access and people that should be allowed access will be blocked out. These are two separate problems, with separate implications. The conse-

---

53. *Id.* at 10.

54. *Id.* at 8; *see e.g.*, EPIC, *Online Guide to Practical Privacy Tools*, http://www.epic.org/privacy/tools.html (accessed May 25, 2004) (some examples of anonymising services).

55. Edelman, 9, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf.

56. Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L.J. 785, 812 (2001); *see also* Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan. L. Rev. 1403, 1405 (1996).

57. Roger Clarke, *Defamation on the Web: Gutnick v. Dow Jones,* http://www.anu.edu.au/people/Roger.Clarke/II/Gutnick.html (accessed May 25, 2004).

quence of false positives can, for example, be that persons at an 'undesirable' location gets access to material that is defamatory under the laws in effect there, or that a contract is entered into with a person at an 'undesirable' location. The consequences of false negatives are essentially twofold; the Web site operator misses out on some access-seekers, and access-seekers misses out on some Internet content.[58] Thus, from a legal perspective, false negatives are only a concern if a person is prevented from accessing material he/she has a legal right to access (i.e. a fee-based subscription-service), or if they occur in a discriminatory manner.[59] To this problem there is a possible solution. Any inconvenience caused by false negatives can be lessened by the Web site operator providing access-seekers with the possibility to contact him/her if feeling unfairly prevented from accessing the site in question. Further, operators of fee-based subscription-services would be well-advised to take extra care in the registration of users. At that stage, the subscriber could easily be asked to identify the location from which he/she accesses the Web site, or perhaps even better, his/her habitual residence. The conditions could further state that the service will only be provided to the access-seeker when he/she is physically located in states A, B and C, and no breach of the subscription contract would occur.

False positives are somewhat more difficult to address. However, if a person gets access that should not be allowed access, the Web site operator could still be protected against any legal responsibility related to that false positive, as he/she, by adopting the best current technology, has taken the steps available to avoid such access. Whether or not the Web site operator should enjoy such immunity based on the application of geo-location alone is, however, a question for the regulators. Perhaps Web site operators should be taking further steps to limit the risk of false positives. Many, not to say most, geo-location technologies provide an estimation of the accuracy in each individual case. If that estimation illustrates a high risk of inaccuracy, the Web site operator could take additional steps to verify the location of the access-seeker. In the *Yahoo!* case, it was suggested that those users who could not be associated with an accurate geographical identification through an IP analysis, for example due to anonymising technologies or proxy servers, could be requested to declare their nationality.[60] However, one of the experts expressed

58. Of course, the Web site operator would be likely to suffer the loss of individual access-seekers, if they repeatedly are refused access. While such errors probably will lead to complaints, possibly increased service costs and arguably result in a negative impact upon the Web site's image, the risk of errors may also work to make the Web site operator anxious to obtain the most accurate technology available (which is not a bad thing in itself).

59. That kind of complication is beyond the scope of this discussion.

60. *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.*, County Court of Paris, interim court order

some concern about the efficiency of this approach.[61] First, he suggested that "users can choose to lie about their locations"; secondly, "every user of the Web site would have to be asked to identify his or her geographical location since the Web server would have no way to determine a priori whether the user is French or is using the Internet from a French location";[62] and thirdly, as some users delete cookies,[63] the users may have to be asked repeatedly for their location. While at least the first and the third concern raised by the expert must be taken into account, it would still seem that self-identification may be usefully applied as a compliment to geo-location technologies. If a Web site operator has taken appropriate steps, such as the application of geo-location technologies, to avoid contact with a certain location, and he/she is subjected, for example, to an action in defamation, at that location, the action might not be allowed.[64] Either way, even if an action in defamation were allowed, the damage done would potentially be minimised, as only a very small number of people at the undesirable location would have been able to gain access to the defamatory material. Finally, it is worth noting that the implications, or at least the severity of the implications, of false positives and false negatives depend on the manner in which geo-location technologies are applied. If used to allow access only to a relatively small group of people (e.g. people located in New Zealand, but not to people located anywhere else in the world) the percentage of false positives, out of the total number of positives, will be very high. At the same time, the percentage of false negatives, out of the total number of negatives, will be very low. An example can illustrate this point. Imagine that a New Zealand based Web site wishes to broadcast a very popular movie over the Internet. Imagine further that such a broadcast would be legal under the laws of New Zealand, but potentially illegal, as a breach of copyright, elsewhere. Under such circumstances, the Web site operator may wish to restrict the access to people located within New Zealand. Let us assume that both the sensitivity (true positive rate) and the specificity (true neg-

---

of 20th of November 2000 (English translation available *at* http://www.cdt.org/speech/international/001120yahoofrance.pdf (accessed May 25, 2004).

61. *See* Vinton Cerf's comments in *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.*, County Court of Paris, interim court order of 20th of November 2000 (English translation available *at* http://www.cdt.org/speech/international/001120yahoofrance.pdf (accessed May 25, 2004).

62. This does not seem correct. Only the ones who cannot be identified by the use of sophisticated geo-location technologies would have to provide identification information. This is, of course, unless the information gained through self-identification is to be used to cross-check the location identified by the applied geo-location technology.

63. The idea was to place a cookie on each user that has identified their location, to avoid repeated identification requests.

64. This way of thinking was certainly the rationale in the French *Yahoo!* decision.

ative rate) of the applied geo-location technology is eighty percent on a country-level. Assume that, due to the popularity of the broadcasted movie, 100,000 people try to access the relevant Web site, and that out of them, only 5,000 are actually located in New Zealand. The result would be that 4,000 people located in New Zealand would correctly get access (true positives), 1,000 people located in New Zealand would incorrectly be denied access (false negatives), 19,000 people located outside New Zealand would incorrectly get access to the Web site (false positives), and 76,000 people located outside New Zealand would correctly be denied access (true negatives). Thus, no less than 82 percent of those who did get access to the relevant Web site would be located outside New Zealand and consequently should not have been getting access. If we change the example somewhat and instead say that the broadcasting of the movie would only be illegal in perhaps one state (e.g. the U.S.), the result is quite different. Out of the 100,000 who tries to access the Web site we can, for example, say that 20,000 are from the U.S. (and should not be getting access). Under such circumstances, 64,000 people would correctly get access, 16,000 people would incorrectly be denied access, 4,000 people located in the U.S. would incorrectly get access and 16,000 located in the U.S. would correctly be denied access. Thus, the percentage of false positives amongst those who got access would be very small (under 6 percent), while 50 percent of those who where denied access should have been allowed access.

Bearing in mind that the occurrence of false negatives ordinarily is a less serious problem, at least from a legal angle, it would seem preferable for Web site operators to apply geo-location technologies in a manner that excludes undesirable locations rather than in manner that only allows access to desirable locations. On the other hand, such a approach would require that the Web site operator was in a position to single out the undesirable locations, which of course requires more, and wider, legal knowledge than simply identifying one or some desirable locations.

In light of the above, it would seem that the courts must accept a rather high percentage of false positives when evaluating a Web site operator's use of geo-location technologies to exclude access by all but the access-seekers from a particular state, or group of states. Indeed, to ensure that Web site operators in such situations are effectively protected, courts may have to look beyond the leakage and view the use of geo-location technologies alone, as a sufficient indication of an intention to avoid contact with undesirable forums. Connecting this line of reasoning to U.S. law, for example, the courts could take the approach that, if a Web site operator has adopted a geo-location technology, with a reasonable degree of accuracy, there can be no minimum contact between the Web site operator and the locations he/she has been trying to avoid com-

ing into contact with, even if he/she did in fact come into contact with that location due to leakage in the geo-location technology.

3. *The Future of Sophisticated Geo-location Technologies*

It is submitted that the development and improvements of sophisticated geo-location technologies has now gained the sort of momentum that makes it very difficult to stop. Even disregarding the forces of commerce that may have originally brought these technologies about, the fact that courts have started to take account of geo-location technologies is, as noted above, a huge incentive for continued development. This, in turn, is likely to lead to improved accuracy, and this improved accuracy can motivate courts to place an even heavier emphasis on these technologies. To be a bit poetic, the wheels of geo-location technologies are in motion, and the consequences for Internet Web site operators are significant:

> It will leave them with a choice: to publish freely and accept legal accountability; to keep some material off the Internet entirely, for fear of criminal and civil charges filed in different countries or even different states; or to give access only to certain viewers, by installing on-line gates and checkpoints around their sites.[65]

Of course, a Web site operator must not necessarily take an "all or nothing" approach. In many, not to say most, cases the better approach would be to make the Web site available globally, but restrict access in relation to those sections of the site that may contain controversial material.

As to the future, it is interesting to note that the Internet Engineering Task Force is working towards the introduction[66] of a new version of the Internet Protocols. The current version IPv4 is to be replaced by IPv6.[67] It has been said that the introduction of IPv6 would enhance the accuracy of geo-location technologies. In fact it has been said that IPv6 would make the identification of the physical location of an Internet user a rather trivial task.[68] "IPv6 [. . .] would expand the IP address system and make people more easily identifiable by assigning serial numbers to

---

65. Matthew Fagin, *Regulating Speech Across Borders: Technology vs. Values*, 9 Mich. Telecomm. & Tech. L. Rev. 395, 414-415 (2003).

66. While already in limited use, IPv4 is still, by far, the dominating internet protocol in use.

67. *See* Stephen E. Deering & Robert M. Hinden, *Internet Protocol, Version 6 (IPv6) Specification* (December 1998), http://www.ipv6.org/specs.html (accessed May 25, 2004) (providing detailed technical information about IPv6).

68. Stefanie Olsen, *Geographic Tracking Raises Opportunities, Fears*, http://news.com.com/Geographic™racking®aises+opportunities%2Cêars/2100-1023_3-248274.html (accessed November 8, 2000).

each computer's network-connection hardware."[69] On the other hand, it has also been suggested that IPv6 might make geo-location technologies less accurate:

> [IPv6] will allow ISPs to dynamically reassign their address ranges at any time. The process for IP address reassignment is rather cumbersome under IPv4 due to the need to reconfigure routers and servers, and therefore they do not happen with anywhere near the frequency that is expected under IPv6, which will make the reassignment of IP address far easier to accomplish. With no actual geographic constraint, under IPv6 these IP address blocks could be reassigned to a new area at any time that demand shifts. As the Internet continues to expand and the need for renumbering grows, blocks of IP addresses will be shifted geographically with increasing regularity. Keeping track of all the growing number of reassignments of IP addresses may overwhelm geolocation software's capabilities. Moreover, during the multi-year global transition to Ipv6 [sic], dual sets of router table data will have to be maintained for both Ipv4 [sic] and Ipv6 [sic] IP addresses. The need to translate and correlate between tables may also introduce latency that negatively impacts the ability to conduct real time analysis.[70]

In light of this, it would seem there are reasons to think that while some aspects of IPv6 might work to enhance the accuracy of geo-location technologies, other aspects will work to decrease the accuracy of these technologies.

On a more general level, it has been suggested that the future accuracy of geo-location technologies will be lower rather than higher, when compared to today's figures. In this context, it is interesting to observe Edelman's thoughts on the future: "Looking forward, there are significant reasons to expect it to become harder, not easier, to produce accurate geographical analysis tools and to thereby restrict retransmitted over-the-air- television content to a Canadian audience."[71] Edelman makes no mention of the prospective effects of IPv6, and it should perhaps be remembered that his Declaration was written on behalf of the National Association of Broadcasters, in relation to a Canadian discussion paper regarding the retransmission of over-the-air television on the

---

69. Patricia Jacobus, *Building Fences, One by One*, CNET news.com, April 19, 2001; *see also* Joel R. Reidenberg, *Yahoo and Democracy on the Internet*, 42 Jurimetrics J., 261 at 263 (2002).

70. Information Technology Association Of America, *ECommerce Taxation and the Limitations of Geolocation Tools*,at 7 http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf (accessed May 25, 2004); *see also* Howard Kim & Simon Dobson, *An Improved Approach to Geographically Locating Web Clients*, http://www.cs.tcd.ie/publications/tech-reports/reports.01/TCD-CS-2001-49.pdf (accessed May 25, 2004) (briefly mentioning that the change to IPv6 "will make the maintenance of the mappings extremely difficult.").

71. Benjamin Edelman, *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-Air Television Content to Canadian Internet Users*, 11, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (accessed May 25, 2004).

Internet.[72] The reasons he relies on are, however, persuasive and include a perceived rise in the deployment of proxy servers, tunnelling systems, and terminal services, an increase in the deployment of mobile network devices, and a likely increase in the availability of automated tools or generally known methods for circumventing geo-location technologies.[73]

But the geo-location technologies discussed above are not the only alternative. Both the methods of soft protection discussed further below, and unsophisticated geo-location technologies must be considered if we are to properly evaluate the potential role for the sophisticated geo-location technologies discussed above.

B. Unsophisticated Geo-location Technologies

When a 'Web surfer' accesses a Web site, his/her browser provides the Web site, or rather the server hosting the Web site, with a wide range of information, the extent of which probably would surprise many Internet users. The Web site *can* receive the following information that can be used for geographical identification:[74]

Language setting – The computers language setting often provides a very accurate geographical identification on a country level. Not only does it work with languages with limited geographical spread, such as Swedish, but also since there are, for example, no less than thirteen[75] versions of English to choose from, identification can take place within a geographically widespread language, such as English. It is often said that one of the prime benefits of sophisticated geo-location technologies is that the Web sites can be presented in the user's preferred language, but it would seem that such a result could be obtained already with unsophisticated methods like this;

Time zone/time display – The browser also provides information about the user's time zone setting and how the local time is displayed. The geographical accuracy of the time zone setting varies, of course. While the setting for Sydney also includes Canberra and Melbourne (and thus clearly specifies Australia), the time zone setting for, for example, Helsinki also include Kiev, Riga, Sofia, Tallinn and Vilnius (and thus

72. The National Association of Broadcasters was, for obvious reasons, opposing the retransmission of over-the-air television on the Internet, and the lack of accurate geo-location technologies was at the centre of attention in the debate.

73. Benjamin Edelman, *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users* 11, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (accessed May 25, 2004).

74. The extent of the information provided varies between different browsers and different versions of those browsers, and may also depend on the settings at the server; *see* Consumer.Net, *Homepage*, http://www.consumer.net/IPpaper.asp (accessed May 25, 2004) (explaining what information is provided in an access request).

75. Windows XP (Home edition).

specifies no less than six countries).[76] Furthermore, also the user's preference in how the local time is displayed can give some, although limited, indication as to geographical origin (e.g. the use of the AM/PM system); and

LOCATION – In at least some systems, such as Windows XP, the user also has the opportunity to specify his/her location. This information is used to get the desired content on certain Web sites that are set to provide localised content (e.g. MSN), but can of course be used also for other geo-identification purposes.

All this combined could give a fairly accurate picture of the access-seeker's geographical location, but the unsophisticated geo-location techniques are easy to circumvent and thus carry limited value in some contexts.

C. GEO-LOCATION TECHNOLOGIES IN PRACTICE

As already mentioned, the application of geo-location technologies was a central topic in the *Yahoo!* case, and the perceived lack of geo-location technologies was arguably determinative in *Macquarie Bank Limited & Anor v. Berg*. However, the technology has also been touched upon in other court cases. In the Supreme Court of Victoria's decision in the *Gutnick* case, Hedigan J apparently was of the view that a Web server can distinguish between different users' requests based on their physical location.[77] It is very unfortunate that Justice Hedigan did not provide any support for his conclusion, or indeed, discuss the controversial issues associated with such practice. Further, the matter was not discussed in the subsequent High Court judgment. However, in this context it is interesting to note that the defendant, Dow Jones, maintained their 'chilling effect' argument also in the High Court continuing to argue that if foreign publishers, like Dow Jones in this case, are subjected to Australian courts and Australian defamation laws, there is a risk that the foreign publishers can choose to prevent Australians from accessing their material. In support of this, Mr. Robertson, representing Dow Jones, convincingly illustrated that there may be very little economic incentive for foreign publishers to enter the Australian market:

> There are 300 subscribers who pay $59 for the right to subscribe to this valuable business web site. That comes in at about $US18,000 and of course there are a lot of deductions, so I guess about $12,000 is accrued from Victoria. [. . .]Your Honour, in terms of a hard-nosed publisher in

76. In reality there are, of course, also other states within the same time zones. However, it would seem possible that the time zone setting not only reveals the actual time zone but the specifications selected by the user, which would limit the possible states identified through the time zone setting.

77. *Gutnick v. Dow Jones & Co Inc.* [2001] VSC 305 ¶¶ 19, 41, and 42, http://www.austlii.edu.au/au/cases/vic/VSC/2001/305.html (accessed May 25, 2004).

> America with that sort of figure saying, "Well, if Justice Hedigan's judgment says we can avoid massive legal costs of being sued in Victoria *simply by not taking Victorian subscribers or by erecting a firewall, but it won't work, let's do it.*"[78] (emphasis added)

With this in mind, it certainly seems clear that some publishers may have convincing reasons to attempt to prevent, for example, Australians from accessing their material. Such practice becoming common, is obviously highly undesirable for the people of Australia. However, the quote also illustrates a weakness in Dow Jones' arguments. While calling attention to the risk of Australians being prevented from accessing Internet material, Mr Robertson was also trying to emphasise that there are no effective means for preventing access-seekers based on their geographical location – an obvious contradiction.[79] A similar 'double-standard' can be seen in the *Yahoo!* case. While arguing that it was not possible to distinguish between users based on their location, *Yahoo!* was providing geographically targeted advertisement on its auction site.[80] This could be interpreted as an indication that, while many Web site operators would prefer not to restrict access based on geography, they are keen to adopt the business advantages that geo-identification provide.

III. SOFT PROTECTION – NON-TECHNICAL MEANS OF GEOGRAPHICAL IDENTIFICATION

In evaluating the need for geo-location technologies, we must bear in mind the possible alternatives. There are also non-technical solutions for geographical identification. In fact, as pointed out by Goldsmith/Sykes:

> It is a mistake to claim that web content providers cannot control content flows on the World Wide Web. They frequently do this by conditioning access to content on the presentation of payment information. They can also condition access on the presentation of geographical or age identification. The process of conditioned access can, of course, be costly. If a content receiver must establish geographical identification by sending the content provider a facsimile, or establish age identification by mailing to the content provider a copy of a driver's license, the process of content distribution slows significantly. [. . .] The point for now is that

78. Transcript of High Court hearing of *Dow Jones & Company Inc v. Gutnick*, 28th of May 2002, points 3552 – 3563, http://www.austlii.edu.au/au/other/hca/transcripts/2002/M3/2.html (accessed May 25, 2004).

79. The suggestion that Web sites are unable to determine the geographical location of access-seekers constituted a fundamental part of Dow Jones' arguments.

80. *International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v. Yahoo! Inc.*, County Court of Paris, interim court order of 20th of November 2000 (English translation available at http://www.cdt.org/speech/international/001120yahoofrance.pdf (accessed May 25, 2004).

> the pertinent issue is not the *impossibility* of geographical and age identification and filtering, but rather the *cost* and *effectiveness* of these services.[81] (footnotes omitted)

These non-technical means of identifying the geographical location of those active on the Internet can suitably be grouped together as 'soft protection', as opposed to the 'hard protection' provided by strictly technical solutions. To a large extent, these means for soft protection rely on information wilfully provided by the access-seeker. The ITAA report on geo-location technologies concluded that:

> The ability to rely on customer declared information regarding the physical location or country of residence (depending on tax type) is, at present, the best interim approach for e-commerce vendors. Furthermore, the decision to use geolocation software – now or in the future, or possibly successor technologies that may provide a better quality of information at a lower cost, is something that should be left up to individual businesses; it would be inappropriate for governments to mandate their use for tax or any other purpose.[82]

Furthermore, a recent survey illustrated that:

> The most popular approaches to identify users were through user registration or self-identification. Passwords, credit card matching, cookies, and geo-identification technologies were all relatively rare methods of identifying user location. Consistent with the greater concern for jurisdictional risk, the media sector ranked first amongst all sectors in seeking to identify user location, while North American respondents (69 percent) were far more likely than either Asian (41 percent) or European (29 percent) to implement identification measures.[83]

Against that background, it is not only interesting, but of fundamental importance, to examine what alternatives to the application of geo-location technologies are available. After all, many, not to say most, of the soft protection methods outlined and discussed below, are both cheaper and easier to implement than the methods of hard protection discussed above.

A. DISCLAIMERS

Disclaimers, or terms of use, have been used with varying success, and for a range of purposes. Since a Web site can be accessed from anywhere in the world and thus have potential legal consequences in any

81. Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L.J. 785, 809 (2001).

82. Information Technology Association Of America, *ECommerce Taxation and the Limitations of Geolocation Tools* 7, http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf (accessed May 25, 2004).

83. Michael Geist, *et al.*, *Global Internet Jurisdiction: The ABA/ICC Survey* (April, 2004), http://www.mgblog.com/resc/Global%20Internet%20Survey.pdf (acessed May 25, 2004).

state, businesses have in many cases taken measures to limit those consequences by placing legal disclaimers on their Web sites. A disclaimer could, for example, state that only persons from a particular state were allowed to access the Web site in question.

Great variations exist from state to state in terms of the extent to which a disclaimer may be upheld. To construct one disclaimer that would be globally effective is probably impossible and would, of course, be very costly since it would require knowledge of every legal system in the world. Another problem is language. A disclaimer written in Swedish, for example, would probably have little effect in relation to an Australian citizen (particularly in an Australian court, under Australian contract law).

The legal validity of disclaimers has been discussed in several cases. For instance, in Australia, they have been held to have some value, for example, in relation to section 52 of the *Trade Practices Act* 1974 (Cth).[84] But it is clear that their value is predicated on their being adequately brought to the attention of the persons to whom they are addressed.[85] Further, it is clear that the weight given by a court to disclaimers will depend on an assessment of all of the circumstances of the particular case.[86] In relation to a territorial disclaimer, for instance, a court is unlikely to attach much weight to a statement on a Web site stipulating 'Intended for UK residents only', when the Web site operator targets, for example, Australian users (e.g. by sending e-mail advertisements to the latter).

In the U.S., it has been held that simply including a disclaimer on a Web site does not necessarily bind the visitors to the terms and conditions stated in the disclaimer: "It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site."[87] Similarly, it has been held that an invitation to agree to a license agreement did not bind the users as they could download the software in question, without affirming their agreement to the terms of the license agreement.[88]

---

84. *See Motor Accidents Authority of New South Wales v. North Cronulla Investments Pty. Ltd.* [1999] FCA 972.

85. *Britt Allcroft (Thomas) LLC v. Miller* [2000] FCA 699; see also *Ticketmaster Corp., et al. v. Tickets.com*, 2000 U.S. Dist. Lexis 4553 (C.D. Cal. 2000)

> ("It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site.").

86. *Britt Allcroft (Thomas) LLC v. Miller* [2000] FCA 699.

87. *Ticketmaster Corp., et al. v. Tickets.com*, 2000 U.S. Dist. Lexis 4553 (C.D. Cal. 2000).

88. *Specht et al., v. Netscape Communications Corp.*, 150 F.Supp. 2d 585, (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (S.D.N.Y. 2002).

B. 'CLICK-WRAP' AGREEMENTS

The difficulty of proving that a particular disclaimer has actually been brought to the other party's attention has prompted the use of other solutions. It is common for Web sites to include so-called "click-wrap" agreements (i.e., non-negotiated contracts of adhesion that normally are entered into when one party clicks on the "I agree" or "Accept" button on a Web site). Typically, an access-seeker is presented with a more or less extensive list of clauses and has to, without the opportunity of negotiations, either accept or decline to proceed with whatever the contract relates to. However, one also finds combinations of click-wrap agreements and disclaimers. For example when accessing ABSOLUT VODKA's Web site, you are asked whether you are of legal drinking age, and are presented with the two alternatives "YES" and "NO" (in four times as large font). This must, of course, be classed as a click-wrap agreement. But, looking more carefully one can also see that in a font less than half the size of the question, and approximately a tenth of the size of the answer alternatives, it is stipulated that "by clicking on yes, you agree to the terms and conditions of this site." To read those terms and conditions one has to click on a link that takes you to a Web page outlining all terms and conditions.

There is only a limited amount of case law on this type of contracts of adhesion, and different courts have taken different approaches. Sometimes the click-wrap contract is held to be valid, and sometimes not.[89]

89. *See Caspi v. Microsoft Network, L.L.C.*, 323 N.J.Super. 118 (N.J. Super. Add. Div. 1999) (exemplifying the U.S. courts' reasoning in relation to so-called "click-wrap contracts). There the plaintiffs had brought a class action against Microsoft in relation to a unilateral change to the membership fees of the defendant's service "MSN". *Id.* The click-wrap contract stated that the agreement was governed by the laws of the state of Washington and that Washington courts had exclusive jurisdiction. *Id.* In evaluating the validity of the contract, the court noted that the plaintiffs' consent did not appear to be the result of fraud. *Id.* Further, as "[t]he on-line computer service industry is not one without competition, and therefore consumers are left with choices as to which service they select" the plaintiffs "were not subjected to overwhelming bargaining power in dealing with Microsoft." *Id.* The court also noted that: "In order to invalidate a forum selection clause, something more than merely size difference must be shown. A court's focus must be on whether such an imbalance in size resulted in an inequality of bargaining power that was unfairly exploited by the more powerful party." *Id.* (citing *Carnival Cruise Lines v. Shute*, 499 U.S. 585 (1991) and *Hodes v. S.N.C Achille Lauro Ed Altri-Gestione*, 858 F.2d 905 (3d Cir. 1988), cert. denied (490 U.S. 1001 (1989)) (reference omitted). After this, the court went on to examine whether the choice of forum clause contravened public policy, and whether the enforcement of the choice of forum clause would inconvenience a trial. *Id.* Finally, the court examined the plaintiffs' claim that they did not receive adequate notice of the forum selection clause. *Id.* In doing so, the court noted that "there was nothing extraordinary about the size or placement of the forum selection clause text", thus, to conclude that the plaintiffs were not bound by the choice of forum clause "would be equivalent to holding that they were bound by no other clause either, since all provisions were identi-

That is no different than with other forms of contracts and electronic contracting, as such, has been recognised for many years now.[90] What is important to remember is that there is no general rule against this relatively novel way of forming contracts. The problem, however, is that more often than not, people in general, and arguably consumers in particular, simply do not take the time to read the agreement and do not have the knowledge to adequately understand the implications of the agreement. In research done on this topic, ninety percent of the respondents indicated that they never read the whole agreement, while at the same time sixty-four percent indicated that they always click "I agree." Furthermore, fifty-five percent did not believe that they entered into a legally binding contract when clicking "I agree"![91] One can thus rightfully question the value of using click-wrap agreements to identify the location of access-seekers.

C. MENUS – THE BETTER AND WORST ALTERNATIVE

From the perspective of conflict of laws, a preferable non-technical solution for Web site operators is the option of including a menu, on the Web site, in which the access-seeker must identify from which state he/she is accessing the Web site in question. It could be stated, on the Web site, that only people from the countries in the menu would be allowed to interact with the Web site. That way, a business could accurately and cost-effectively control which forums it exposed itself to. In practice, this option has not been widely utilised, however, menus have been used to provide the most relevant content for the access-seeker. For example, the online job database, www.monster.com, asks where the access-seeker is from and where he/she is going (i.e., where he/she wants to work).

There are at least two advantages with this approach, when compared to disclaimers and click-wrap contracts. Both advantages stem from the fact that the access-seeker has got to take some positive action, more than simply clicking "I agree." First, as this is done, the Web site operator is provided with a clear indication that the access-seeker has, indeed, noticed the requirement in question. The evidentiary value of

---

cally presented." *Id.* (citing *Rudbart v. North Jersey Dist. Water Supply Comm'n*, 127 N.J. 344, 351-53 (N.J. 1992). The court stated that: "Plaintiffs must be taken to have known that they were entering into a contract; and no good purpose, consonant with the dictates of reasonable reliability in commerce, would be served by permitting them to disavow particular provisions or the contract as a whole." *Id.*

90. *See e.g.* the U.S. Electronic Signatures in Global and National Commerce Act (15 U.S.C. § 7001 et. seq.) (effective October 1, 2000); the Australian Electronic Transactions Act 1999 (Cth.) s. 10; and the People's Republic of China's *Contract Law of the People's Republic of China* (1999), Article 11.

91. Adam Gatt, *The Enforceability of Click-wrap agreements*, Computer Law & Security Report Vol. 18 No. 6, at 408.

this must surely be greater than a simple click on "I agree" or the like. Secondly, as the access-seeker is provided with a more active role, he/she is more likely to be aware of what he/she is agreeing to, or certifying, or whatever the aim of the menu is.

On the other hand, from the perspective of Internet development, the use of menus could represent a serious step backwards. One of the main features of the World Wide Web, making it different from previous Internet applications, such as Gopher,[92] is the possibility of "deep-linking." If all links were directed to a portal page, at which the access-seeker had to identify himself/herself, this highly valuable feature would be lost. Imagine, for example, the Australian National Native Title Tribunal's Web site[93] being unable to deep-link to the relevant court decisions, but instead having to link to Australasian Legal Information Institute's (AustLII) portal page. Or, picture a situation where search engine results were not directly accessible, and instead you could only click your way to the portal pages. Then again, it could, of course be argued that, only Web sites containing potentially unlawful material would have to use the menu system. While such an observation would seem to motivate a Web site such as AustLII not to use menus, it must also be remembered that there is a significant divergence in what is considered unlawful amongst the different countries and Web sites might choose to use menus just to be on the safe side. However, one could, of course, picture technical solutions providing for what could be called conditioned deep-linking. Instead of transferring the access-seeker to a portal page at which he/she has to identify himself/herself, the technical set-up could still let the access-seeker access the desired material directly, after the identification has taken place. That way, the technical harm done by the menu system would be minimised.

Based on the above, it can be concluded that a widespread use of menus would inevitably detract from the technical possibilities of the WWW. This highlights that, what might seem like sensible legal solutions, can have a devastating effect, not only on future Internet uses, but also on existing applications. In the end, we have to make a value-decision; does the value of menu usage outweigh the harm it inevitably causes? Without drawing any further analogies, it can be noted that this

92. What Is, Look it Up, www.whatis.com (giving definition of gopher: "From about 1992 through 1996, Gopher was an Internet application in which hierarchically-organized text files could be brought from servers all over the world to a viewer on your computer. Especially in universities, Gopher was a step toward the World Wide Web's Hypertext Transfer Protocol (HTTP), which effectively replaced it within a short time.") (accessed May 25, 2004); *see also* SearchWebServices.com, *Whatis.com Definitions*, http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212203,00.html (accessed May 25, 2004).

93. National Native Title Tribunal, *Homepage*, http://www.nntt.gov.au (accessed May 25, 2004).

type of question, 'does the legal-social benefits outweigh the technical-social disadvantages?' are rather common (e.g., does the legal-social benefits of built-in speed limitation on trucks outweigh the technical-social disadvantages?).

D. Delivery Address

While often overlooked, contractual relations involving physical delivery of goods or services inherently involve a fairly accurate means of geo-identification, as the buyer would have to specify a delivery address. Problems can, however, arise if the delivery address is different from the buyer's location. In addition, no physical delivery address is necessary in contracts for so-called 'digital products.'[94]

E. "Offline Identification"[95]

In his cleverly titled article, "Is There a There There,"[96] Michael Geist discusses another category of soft protection – what he refers to as "offline identification." The most obvious example of this form of soft protection is identification based on credit cards. Credit cards can be used as verification for several purposes such as age and to an extent location:

> As anyone who has purchased online with a credit card knows, the verification process includes an offline component, as the address submitted by the user is cross-checked with the address on file to confirm a match prior to authorization of the charge. This process provides Web sites with access to offline data such as the user's complete address – which is confirmed through a third party, the financial intermediary.[97] (footnotes omitted)

But as noted by Geist, this form of verification has profound privacy implications. In addition, its practical value is limited as not everybody feels comfortable stating credit card information on the Internet. As the users' awareness increase, the value of this form of identification will presumably decrease. In addition, the inconvenience of this sort of identification could be prohibitive in relation to free access Web sites.

---

94. A digitised product is a product that has been transformed from a physically tangible object to a purely digital combination of binary code (e.g. electronic books), or a product that has been removed from its physically tangible carrier and is kept as a purely digital combination of binary code (e.g. mp3 files, MPEG videos and software).

95. Michael Geist, *Is There a There There? Towards Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech. L. J. 1345 at 55 (2001) (stated page number refers to PDF version available at http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf (accessed May 25, 2004) (explaining term as used by Michael Geist).

96. *Id.*

97. *Id.*

F. Soft protection in Practice

In contrast to sophisticated geo-location technologies, neither of the approaches, discussed in this part, could be said to effectively block out anybody as the access-seeker, generally, very easily could provide false information. Consequently, the extent to which the different forms of soft protections actually provide protection for the Web site operator and the access-seeker would reasonably have to be dependent on their respective good faith. In examining the access-seeker's good or bad faith, we can note that in contractual relations, a policy decision needs to be made. One alternative would be to say that the party nominating a fraudulent location lose any right associated with that location and/or his/her real location.

For example, a consumer claiming to be located in state A to get access to a certain Web site, but in realty is located in state B, could lose any consumer protection afforded under the rules of state B, as the seller was not aware of state B's involvement in the transaction, and perhaps had taken steps to avoid that forum. The question is, however, if the consumer in such a situation should also lose any rights provided for under the laws of state A? After all, the seller was aware of the buyer's claim to be located in state A, and would consequently have taken any rights provided for under state A's legislation into account. On the other hand, if the consumer could enjoy the rights provided to consumers in state A, it would mean that a consumer could nominate which states' protection he/she wanted to apply in the transaction. This problem can, of course, be addressed in a number of ways. One example would be to say that, a consumer that has provided false information, in relation to his/her domicile, location or residence, in order to mislead a Web site operator, can only enjoy the least favourable consumer protection laws out of the possible ones (i.e. the ones that would apply based on the consumer's actual domicile, location or residence, and the ones that would apply based on the domicile, location or residence the consumer stated).

As far as the tort of defamation is concerned, access-seeker's bad faith may, of course, render soft protection methods vulnerable or even useless, but for deciding, for example, whether or not a Web site operator has taken reasonable steps to avoid contact with a certain forum, it would be more appropriate to focus on whether or not the operator has acted in good faith. Generally speaking, it would seem reasonable to suggest that a Web site operator could only rely on soft protection if the implementation of hard-protection is unpractical for some reason.

The sort of soft protection that has been discussed above has not always been recognised as sufficient by the courts. One of the more noteworthy cases involves a Canadian Web-company, iCraveTV, which provided its users with the opportunity to view real-time TV via the

company's Web site.[98] Being aware of the fact that, while their activities were arguably legal at the time in Canada,[99] they might have been illegal elsewhere, iCraveTV applied some of the forms of soft protection discussed above. When accessing iCraveTV's Web site, the access-seekers had to enter their local area code. If this area code was not a Canadian local area code, the access-seeker was refused access. This step is, of course, very similar to the menu system discussed above. However, as noted by Geist, this step for geographical restriction could be viewed "as rather gimmicky" as the local area code of Toronto, iCraveTV's place of business, was clearly stated on the site.[100] Having entered a valid Canadian local area code, the access-seeker had to certify being located in Canada by clicking on an "In Canada" icon in a click-wrap agreement. In the third and last access step, the access-seekers had to click "I agree" on another click-wrap agreement, containing the full terms of use (including a verification of the fact that the user was located in Canada). Despite these steps to ensure an exclusive Canadian group of users, a U.S. court claimed jurisdiction over iCraveTV, which was sued by a group of broadcasters, movie studios and sports leagues.[101] Having seen that a U.S. court found itself to have jurisdiction, it is no surprise that the Canadian company lost the case.[102] The *iCraveTV* case illustrates that the value of

98. *See generally Twentieth Century Fox Film Corporation, et al., v. iCraveTV, et al.*, 2000 U.S. Dist. LEXIS 11670; 53 U.S.P.Q.2D (BNA) 1831 (Decided February 8, 2000).

99. Under Canadian law, as it then stood, Internet retransmission of over-the-air television was allowed under certain condition and provided that the retransmission was for Canadians only. The important aspect of this is, of course, that no copyright restrictions were attached to the retransmission. However, a change (Bill C-11, adopted in 2002) to section 31 of the Copyright Act (CA) created an "Internet carve-out" in relation to the compulsory licence regime. *See* further Broadcasting Public Notice CRTC 2003-2 (Ottawa, 17 January 2003); for a detailed discussion of the legality of iCraveTV's operation see Michael Geist, *iCraveTV and the New Rules of Internet Broadcasting,* 23 U. Ark. Little Rock L. Rev. 223 (Fall 2000).

100. Michael Geist, *Is There a There There? Towards Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech. L. J. 1345 (2001), at 6 (stated page number refers to PDF version *at* http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf (accessed May 25, 2004)); *but see* Directive 2000/31/EC on electronic commerce, Article 5(1b-d) (On the other hand, for a company to state its physical address on the Web site could be seen to be good practice, and indeed, is required, for example, under European Community law); *see e.g., Consumer Policy Considerations on the Importance of Accurate and Available WHOIS Data* (June, 2003), http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-cp(2003)1-final (accessed May 25, 2004) (mentioning that efforts along these lines has been made on several levels, such as OECD's work in relation to the accuracy of "WHOIS" data)

101. *iCraveTV is Served Up a Lawsuit*, Wired News, Jan. 20, 2000, *at* http://www.wired.com/news/business/0,1367,33797,00.html (accessed May 25, 2004); Michael Geist, *Is There a There There? Towards Greater Certainty for Internet Jurisdiction*, 16 Berkeley Tech L. J. 1345 (2001), at 5 (stated page number refers to PDF version available *at* http://aix1.uottawa.ca/~geist/geistjurisdiction-us.pdf (accessed May 25, 2004)).

102. *Twentieth Century Fox Film Corporation, et al. v iCraveTV, et al.* 2000 U.S. Dist. LEXIS 11670; 53 U.S.P.Q.2D (BNA) 1831 (Decided on February 8, 2000).

soft-protecting is limited, particularly when it can be argued, that the protection was used in bad faith.

Perhaps as a consequence of the *iCraveTV* case, another Canadian Web-company, JumpTV, set out to rely on hard-protection, in preventing access to non-Canadians. In 2001, it was reported that:

> In order for JumpTV to qualify for a Compulsory Retransmission License (CRL), which would allow it to retransmit the U.S. material for a fee (tarriff), it has to prove that its signal protection software, which restricts access to Canadians-only, actually works. The software is currently under development.[103]

Presently, however, it seems that JumpTV has chosen a different approach. The company provides access to a range of different TV stations on their Web site,[104] and people from anywhere in the world can sign-up (with a monthly fee).[105] Against that background, it would seem that JumpTV has, at least presently, opted for a less controversial approach to online TV-broadcasting.[106]

To summarize the above, the forms of soft protection discussed are all associated with difficulties, and in light of the *iCraveTV* case, do not appear to represent any real alternative to hard protection in the form of geo-location technologies. However, as discussed earlier, soft protection, such as menus and click-wrap agreements, can suitably be used as complements to geo-location technologies.

IV. GEO-IDENTIFICATION – A QUESTION OF ATTITUDES?

Based upon the discussion above, at least sophisticated, geo-location technologies have the power to change the Internet in a very fundamental manner – in the not too distant future, Internet communication may no longer lack reliable geographical identifiers as IP addresses potentially can be seen as reliable indications of geographical location. However, it has been pointed out that reliable technology simply is not enough.[107] Even if geo-location technologies were widely utilised and worked to a satisfactory degree, not all problems associated with the special characteristics of the Internet would necessarily be solved. For example, the simple fact that a Web site operator is aware of the access-

103. James Careless, *JumpTV Fights For Retransmission, at* http://www.digitaltelevision.com/2001/webcast/801_1.shtml (On file with author. No longer available online).

104. As of the 8th of August, 2003.

105. *See* http://www.jumptv.com/site/aboutus_english.ch2 (last visited May 25, 2004).

106. Presuming that JumpTV has entered into some form agreements with the TV stations in question.

107. *See e.g.* Robert Corn-Revere, *Caught in the Seamless Webb: Does the Internet's Global Reach Justify Less Freedom of Speech?*, Cato Institute, Briefing paper N0. 71 (July 24, 2002), at 6; *see also* Roger Clarke, *Defamation on the Web: Gutnick v. Dow Jones,* http://www.anu.edu.au/people/ogerClarke/II/Gutnick.html (accessed May 25, 2004).

seeker's physical location does not mean that he/she can make an informed decision as to whether imparting information to that individual might mean that he/she is at risk of being sued, for example, for defamation in the access-seeker's forum. Bearing in mind the structure of current conflict of laws rules, the Web site operator would need to know both the substantive defamation laws of the location from which the access-seeker is located and that country's conflict of laws rules to make such a decision. Further, since access-seekers may be geographically located virtually anywhere in the world, the Web site operator would arguably have to know all substantial and procedural laws of all the countries on earth – an unrealistic task: Geographic location technology is a red herring." Said Alan Davidson, a lawyer with the Center for Technology and Democracy, a Washington think tank. "It would be incredibly burdensome to tailor content to meet all of the different laws in all of the different countries everywhere in the world."[108]

On the other hand, this line of reasoning appears to be based on the notion that the 'right' or 'ordinary' thing to do, is to use technology to its full potential. Maybe we must depart from such ideas? The publisher of a newspaper, for example, would ordinarily be publishing within a local area, or a country or, if very large, a region. The technology of newspaper publications is such that a newspaper will only be available at those places the publisher has targeted. It could be said that the starting point is zero percent publication-coverage, and for that number to increase the publisher must target a community, country or region with its newspaper. Web publication, on the other hand, works in exactly the opposite way. Once the material is made available on the Web, it has virtually one hundred percent publication-coverage, and for that percentage to decrease, the publisher must take action by 'dis-targeting' undesirable forums.[109] As the appropriate technology becomes available, and economically and practically feasible to use, Web publishers may need to change their way of thinking.[110] Maybe also Web publishers will have to, through the use of technology, take the zero percent publication-coverage as their starting point, instead of the one hundred percent publication-coverage (which could be said to represent full utilisation of the technology)? Maybe Web-publishers will need to choose the market where they feel safe, to the exclusion of all other markets?

---

108. Ariana Eunjung Cha, *Rise of Internet 'Borders' Prompts Fears for Web's Future*, Washington Post, (Jan. 4, 2002).

109. Any proposition to the effect that Internet activities are functionally identical to offline activities fits uneasily with this observation.

110. Indeed, maybe such a change in approach is justified already today with the available technology? Perhaps even the alternatives of 'soft protection', discussed above, justify such a change in approach?

One question that arises from all this is: do we want to give up the advantages of full utilisation of the Internet technology, for the purpose of, for example, being able to sue Web publishers where their material is read? The reality is that people have grown accustomed to being able to access an extremely diverse range of information via the Internet. For example, a Swede living in Australia may appreciate being able to read Swedish newspapers online and listening to Swedish radio broadcasts online. In relation to this, Jack Goldsmith concludes that:

> As cost of such [information flow] control continues to drop, and the accuracy and ease of this control increases, cyberspace content providers will come to occupy the same position as the newspaper publisher. It will thus be appropriate in cyberspace, as in real space, for the law to impose small costs on both types of publisher to ensure that content does not appear in jurisdictions and networks where it is illegal.[111]

If we accept this conclusion, we must necessarily also be prepared to give up a range of privileges we have become used to having – the Internet would in a sense become much more regionalised. At the same time, it must be pointed out that examples can be given, illustrating that the Internet could be invigorated by the use of geo-location technologies. Up until Athens 2004, the Web-coverage of the Olympic Games has been limited to text and pictures in various forms.[112] While you have been able to find impressive statistical data, biographical details about all athletes and various other features, there has been a paucity of audio and video coverage. Over the last couple of years, the International Olympic Committee (IOC) has provided two reasons for this: the "poor quality" of Internet broadcasts and the lack of reliable geo-location technologies.[113] It has been reported that Dick Pound[114] stated that:

> 'Until the technology changes to allow the video to be restricted, we have a problem,' Pound said. 'Historically, we have sold rights in a particular territory. Unless and until you can guarantee that the signal will be restricted to your territory, then you cannot put real time video or real time audio on the Internet.'[115]

The IOC's position on geo-location technologies is nicely summarised by Staci Kramer: "The Olympics may be about tearing down borders but

111. Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. Chi. L. Rev. 1199, 1230 (1998).

112. For a detailed discussion of Olympic broadcasting rights, see: Toby Ryston-Pratt, *Olympic TV Rights*, Communications Law Bulletin, Vol. 21 No. 4 2002, at 12-15.

113. Martyn Williams, *Olympic Games Go for the Gold Online*, http://www.pcworld.com/esource/printable/article/0,aid,83903,00.asp (accessed May 25, 2004).

114. At least at the time of speaking, the chairman of the IOC marketing commission and Internet Work Group.

115. Steve Klein, *Back to the 20th Century: The Olympics and the Internet*, http://mason.gmu.edu/sklein1/ndex_files/contentexchangecolumns/column11.htm (accessed May 25, 2004).

not when it comes to TV territories."[116] However Pound's statement should probably be read in light of the fact that "[t]he IOC earned 51% of all its revenues from the Sydney Games through sale of broadcast rights."[117] Yet, it may also be worth bearing in mind the IOC's historic inability to adopt new distribution mediums: "In 1960, former IOC president Avery Brundage said, 'We in the IOC have done well without TV for 60 years and will do so certainly for the next 60 years, too.'"[118] However, with the increase in broadband use and the improved accuracy of geo-location technologies in mind, IOC-backed Internet broadcasting trials took place in three major Swiss cities, during the 2002 Winter Olympics. Furthermore, streaming video was offered by a number of broadcasters via the Internet during the summer Olympics in Athens 2004.[119]

In light of the above, it would seem that the absence of geo-location technologies is not a guarantee for the full utilisation of the Internet being achieved. In fact it may be unreasonable to talk about any "full utilisation" of the Internet, because full technological utilisation may not lead to actual full utilisation due to regulation restraints. This is a fundamental consideration to bear in mind – the extent of actual utilisation of Internet technology is limited by both technical and regulatory restraints. Furthermore, the Internet is what we make it and it is mainly limited by our imagination. The question should, thus, more correctly be: do the advantages of geo-location technologies outweigh the disadvantages? To re-connect to Lessig's theory of the four regulating mechanisms, it would seem that both the market and the law already have answered this question in the affirmative. It seems that the only remaining question is: how the fourth mechanism, 'norms', will respond?

A. PRIVACY – A SERIOUS OBSTACLE OR SIMPLY A BUMP IN THE ROAD?

Leaving aside the accuracy issues discussed above, there seems to be only one potentially major obstacle to a widespread use of geo-location technologies. If IP addresses are considered 'personal data' or 'personal information' for privacy purposes, the collection, use and disclosure of such information may be seriously restricted. While the developers of

116. Staci Kramer, *Frustration: A New Demonstration Sport*, *at* http://www.ojr.org/ojr/business/1017712999.php (accessed May 25, 2004).

117. Klein, *supra* n. 115.

118. *Id.*

119. IOC Press Release of August 7, 2004, *Global TV viewing set to break records for the Athens 2004 Olympic Games*, *at* http://www.olympic.org/uk/news/media_centre/press_release_uk.asp?id=958 (accessed Aug. 11, 2004); *see also* BBC Sport, *Olympics 2004*, http://news.bbc.co.uk/sport1/hi/olympics_2004/3919855.stm (accessed Aug. 1, 2004) (for an example of making video and audio coverage available to people who live in the UK and have a broadband connection).

geo-location technologies argue that their products are "non-invasive"[120] and "privacy safe,"[121] it is unclear how, for example, courts and authorities will view this issue. As the privacy protection regulation of the European Union is one of the strictest in the world, and has been very influential, it is here suitable to focus on EC law.

In his book, *Data Protection Law – Approaching Its Rationale, Logic and Limits*, Lee Bygrave suggests that it is quite possible that IP addresses *can* constitute personal data as defined in Article 2(a) of the *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)*[122] ("EC Directive").[123] Bygrave identifies three criteria by which the EC Directive determines whether or not information constitutes "personal data":[124]

- "the probability of identification;"[125]
- "the degree of technical ease with which identification can occur;"[126] and
- "the amount of time and effort demanded by the identification process."[127]

As to the first criterion, it is particularly relevant to note that:

> The possibility of a multiplicity of persons sharing a machine with an address registered in the name of only one person is unlikely to disqualify that machine address from being treated as personal data. Many numbers (eg, car registration and telephone numbers) which are formally registered against the name of one specific person tend to be treated as personal data even if the objects to which they directly attach are occasionally or regularly used by other persons.[128]

The first criterion does consequently not seem to exclude the possibility that IP addresses, in the context geo-location technologies, may constitute personal data. As to the second and third criteria, Bygrave notes that the EC Directives definition of personal data focuses on the capability of identification.[129] Thus, the fact that the data is not actually used for identification is irrelevant, and "any answer [as to whether criteria two and three have been met] will have to be continually revised in

120. Digital Envoy, Press Releases, April 9, 2000 http://www.digitalenvoy.net/news/press_releases/2000/pr_040900.shtml (accessed August 11, 2004).

121. Quova's Technical Overview of GeoPoint, http://www.quova.com/technology/uova_tech_whitepaper.pdf (accessed Nov. 18, 2004).

122. Lee A. Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits*, 316 Kluwer Law International 2002).

123. *Id.* at 316.

124. *Id.* at 316-317.

125. *Id.* at 316.

126. *Id.* at 317.

127. Bygrave, *supra* n. 122, at.317.

128. *Id.*

129. *Id.* at 318.

light of technological-organisational developments; data which presently could only be linked to an individual with great difficulty might be linked relatively easily in the near future."[130] In light of this, it is only logical that Bygrave states that "the extent to which clickstream data [such as IP addresses] may amount to personal data under the Directive is a question of fact that is impossible to answer conclusively in the abstract."[131] The fact that some courts have cut back on the literal scope of the personal data/information concept as it is defined in legislation is adding further to the uncertainty.[132]

As mentioned above, the discussion in this part of the article is focused on EC law. However, the possibility of IP addresses being regarded as personal data/information is by no means limited to the European Union. Indeed, an IP address is potentially classed as 'personal information' under U.S. law. While the *Children's Online Privacy Protection Act* of 1998 (15 U.S.C. § 6501) admittedly might not be of particular relevance in the context of geo-location technologies, it may be observed that 'personal information' is given the following definition in Sec. 1302(8):

> The term 'personal information' means individually identifiable information about an individual collected online, including: (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or parents of that child that the Web site collects online from the child and combines with an identifier described in this paragraph.

As this definition includes both telephone numbers and e-mail addresses, both of which may be used by more than one person, there does not seem to be any reason why an IP address could not be an "identifier that the Commission determines permits the physical or online contacting of a specific individual."

In conclusion, whether or not IP addresses used in the context of geo-location technologies constitute personal data under the EC Directive and other relevant law, would appear to rest upon the technical setup of the geo-location technology, and no definitive context-indepen-

130. *Id.* at 317.

131. *Id.*

132. *See e.g. Eastweek Publisher Ltd. and Another v. Privacy Commissioner for Personal Data* [2000] 1 HKC 692 (28 March 2000); *Christopher Harder v. The Proceedings Commissioner* [2000] 3 NZLR 80 (17 July 2000); and *Michael John Durant v. Financial Services Authority* [2003] EWCA Civ 1746 (2003). The lines taken by the courts on 'personal data' in these three decisions are controversial and their legal validity is, at the very least, questionable. However, they do add to the uncertainty that already surrounds the precise meaning of 'personal data' or equivalent concepts.

dent answer can be given. However, it would seem arguable that the higher the accuracy of geo-location technologies, the higher the likelihood that the IP number constitutes personal data (e.g. if a particular geo-location service is accurate down to the street level, it is more likely to be using data classed as 'personal data' than a geo-location technology that only is accurate on a country level).

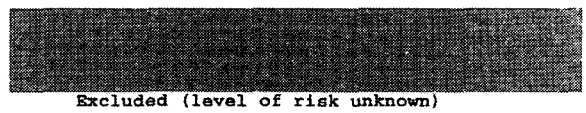
V. CONCLUDING REMARKS

There is an Indonesian saying where novel objects, events or phenomenon are said to be like "hot, hot chicken poo" – hot when first arriving but soon cooling down and being forgotten and of no significance. I think the above has demonstrated that geo-identification and geo-location technologies are much more than "hot, hot chicken poo." In fact, it seems likely that geo-location technologies will contribute to transforming the Internet as we know it into something that more closely resembles our world, so divided by borders of different kinds. However, in evaluating the value of both geo-location technologies and "soft" methods of geo-identification, we must recognise that "the use of such technologies entail a cost – a financial cost to content providers and the social cost of a network that is no longer open and neutral."[133] While such a development is far from ideal, it may nevertheless be unavoidable, and perhaps even the best option. The reality that different states have different substantive laws simply cannot be ignored, and the regulation of activities on the Internet must in one way or another take account of this reality. As long as the rules of conflict of laws focus on the location of the effect rather than on the location of the acting party, there is a huge incentive for Web site operators to know the location of those who access their content, and currently the most effective way of gaining such knowledge is through the application of some form of sophisticated geo-location technology. Thus, the Internet will inevitably transform from a relatively borderless dimension into a medium that takes account of geographical and legal borders. Such a development seem particularly unavoidable when considering how geo-location technologies (as part of architecture/code) affects, and is affected by, the three other forms of regulation. Furthermore, in light of such a development, current "effect-focused" conflict of laws rules may make sense. In other words, from the perspective of Internet regulation, geo-location technologies may, to a large extent, eliminate the regulatory difficulties associated with the Internet's "borderlessness." If it can be assumed that Web content being available in a particular state is an indication of the Web publisher's intention to make the content available in that particular state, the appli-

133. Matthew Fagin, *Regulating Speech Across Borders: Technology vs. Values*, 9 Mich. Telecomm. & Tech. L. Rev.395, 421 (2003).

cation of effect-focused conflict of laws rules make sense. While we must remain alert to their less than perfect accuracy, geo-location technologies have the potential of making such assumptions valid *prima facie*. It would thus seem that discussions of Internet regulation necessarily must take account of these emerging technological solutions. Considering the above, it is submitted that the courts now have a great responsibility in ensuring that the potential of geo-identification is recognised and appreciated. From a practitioners' perspective, geo-location technologies highlights the increasing need for lawyers to be technology-savvy. As far as, for example, e-commerce is concerned, a lawyer needs to be up-to-date with technological solutions, such as geo-location technologies, before legal solutions can be identified and evaluated. Looking at geo-location technologies from the perspective of a legal practitioner advising a client, a few things need to be observed. Case law has illustrated that the methods of soft protection discussed in this article cannot be said to constitute realistic alternatives to the hard protection provided for by geo-location technologies. However, soft protection may usefully be implemented as a compliment to geo-location technologies. Further, as to the actual use of geo-location technologies, there seems to be two alternatives: access to sensitive content can be limited to people from desirable locations (i.e. only people from a limited number of locations get access), or access-seekers from locations identified as undesirable may be blocked from accessing sensitive content (i.e. the content is open to all but the people from certain locations). The following simple pictures may illustrate and help clarify the implications of these two options:

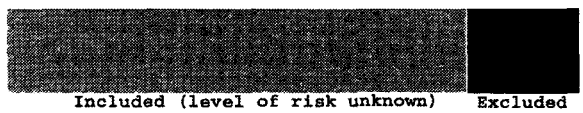
ALTERNATIVE 1



Included (Known free of risk)

Excluded (level of risk unknown)

ALTERNATIVE 2



Included (Known free of risk)

Included (level of risk unknown)

Excluded (Risk known)

In the first alternative, the Web site operator will be faced with a high percentage of false positives and is obviously severely limiting the Web site's exposure. At the same time, this method appears to represent the safer alternative. In the second alternative, the Web site operator is

only excluding people from those locations he/she has identified as high-risk locations. This way, the Web site still gets a high degree of exposure. However, that exposure includes exposure to locations potentially associated with legal risks. Which alternative is preferable will have to be judged in light of the particular circumstances of the Web site in question, and no answer to be given on a general level. To conclude this article, as noted by Mark I. Wilson and his colleagues "[w]hile the power of distance has been eroded, it should not be confused with the diminishing meaning of place."[134] Place, or location, matters offline and matters online. Geo-location technologies 'merely' make it possible and practical to consider location, also online.

134. Mark I. Wilson, *et al.*, *Death of Distance/Rise of Place: The Impact of the Internet on Locality and Spatial Organization* (Paper prepared for Presentation at INET 2001, The 11th Annual Internet Society Conference (Stockholm, 5-8 June 2001).