2-14-2007

"Imagine there's no countries..." – Geo-identification, the law and the not so borderless Internet

Dan J B Svantesson
Bond University, dan_svantesson@bond.edu.au

“Imagine there’s no countries...” – Geo-identification, the law and the not so borderless Internet∗

Dr. Dan Jerker B. Svantesson∗∗

Imagine trying to access you favourite website, and when doing so, being greeted by a message along the lines of: “We know you are in Sydney (Australia). This website is only intended for the people of Norway.”

While having gained little attention so far, technologies making such a scenario possible already exist, are already in use, and the spread of their use is rapidly increasing. Although the so-called geo-location technologies that make this kind of geographical ‘borders’ possible can be circumvented, we are doubtlessly witnessing the Internet undergoing a remarkable change - from the world's first and only ‘borderless’ communications medium to something that much more resembles our physical world divided by borders of different kinds. This has enormous consequences as we are losing one of the greatest benefits of the Internet, its ability to allow people to communicate across borders.

This article examines how, and to what extent, these technologies work. Further, the legal implications of these technologies are discussed, and a few observations are made as to the likely effect these technologies will have on the future structure of the Internet.

How does it work?

While there are several different methods enabling a website operator to identify the geographical location of those who visit a particular website, it is here suitable to focus on the most widely spread sophisticated form of geo-identification – that is, IP based geo-location technologies. These technologies translate IP addresses[i] into geographical locations, by the use of information stored by the provider of the geo-location service.

As the access-seeker enters the appropriate Uniform Resource Locator (“URL”)[ii] into his/her browser, or clicks on the appropriate hyperlink, an access-request is sent to the server operating the requested website. 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[iii]) 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.[iv] Based on the information in this database, the provider of the geo-location service gives the website server an educated guess as to the access-seeker’s location (in some cases down to city-level). 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 website is intended for the people of Australia only", 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 systems.[v] This technology is not necessarily prohibitively expensive for larger website operators, nor does it appear particularly difficult to operate.

The accuracy of these products is, however, difficult to gauge. While the providers indicate the potential accuracy to be very high, "over 99% at a country level and approximately 92% at a city-level"[vi], it should be remembered that they are after all trying to sell a product, and these impressive figures have been criticised.[vii] 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. Common methods of collecting relevant material include, for example, gathering data from registration databases,[viii] network routing information, DNS systems, host name translations, ISP information and Web content.[ix] As discussed in detail by Edelman, all of these sources may provide inaccurate information.[x]

Turning to circumvention problems, it can be noted that, while some circumvention techniques are technologically advanced (e.g. deep linking to streaming video content without accessing the HTTP server[xi]), others are easy enough to be used by virtually anyone (e.g. anonymising techniques[xii]) or even inherent in the system-structure ("tunnelling methods"[xiii]). With this in mind, it will presumably always be possible to circumvent geo-location technologies.

Arguably the easiest way to circumvent the type of geo-location technologies described above, is through the use of so-called anonymisers. Anonymisers are applications designed to allow web-users to visit websites anonymously. As illustrated below, anonymisers act as an added layer – a buffer – between the web-surfer and the websites he/she visits. When a web-surfer uses an anonymiser, his/her IP number is only transmitted to the provider of the anonymiser. He/she is then assigned a new IP number by the anonymiser in relation to any websites he/she visits while applying the anonymiser. It needs to be stressed that these applications were not developed for the purpose of circumventing geo-location technologies. However, by identifying the location of the anonymiser (or, more specifically, the location with which the IP numbers assigned by the anonymiser are associated), one may be able to find anonymisers from the country one wishes to appear to be located in. For example, when using an anonymiser called *The Cloak*[xiv], I was assigned an IP number (216.127.72.7) indicating my location as being the US, while when using an anonymiser called *Anonymouse*[xv], I was assigned an IP number (82.96.100.100) indicating my location as being Germany.

The number of anonymisers available is limited, and thus there are only a limited number of countries one can appear to be located in, using such applications. However, the use of so-called proxy servers opens up further possibilities. A bit simplified, a proxy server is a server that sits between the web-browser and the server being accessed. Thus, just like the anonymisers discussed above, a proxy server acts as a buffer between the web-surfer and the websites visited. The main difference is that while the anonymisers are web-applications, the use of proxy servers are determined by the settings in the web-browser. Using a proxy server to circumvent geo-location technologies, involves two easy steps. First it is necessary to obtain the address (with its port number) of a proxy server from the country you wish to appear to be located in. Then the browser settings must be changed to the obtained proxy address (with its port number). For example, users of Microsoft's Internet Explorer can change their proxy server setting by first clicking on *Internet Options* under *Tools,* and then clicking on *LAN Settings* under *Connections*. A few words of warning must, however, be said in this context. Some proxy servers, and anonymiser, can very well log all information that passes through them. In other words, all the web-surfer's traffic can be accessed by the operator of the anonymiser or proxy server. Thus, it is not advisable to send passwords or credit card details through a proxy server, or anonymiser. Furthermore, it is to be noted that people connecting to the Internet using a computer connected to the network of a larger institution, such as a university or a company, may not be able to use proxy servers in the manner outlined above.

When discussing how the effectiveness of IP based geo-location technologies is affected by the availability of anonymisers and proxy servers, it is to be noted that the producers of IP based geo-location technologies are working to identify the servers providing the anonymising services.[xvi] Once identified, the value of the anonymising tool for circumventing geo-location technologies is obviously limited.

What are the legal implications?

The use of geo-identification has profound legal implications. Indeed, virtually all areas of law are affected in one way or another. Making reference to Australian law, a range of affected areas of law are discussed below.

The area of conflict of laws (or private international law as it is referred to in civil law countries) is concerned with three things: When can a court exercise jurisdiction over a defendant? Which substantive law should be used to resolve the dispute? And, under which circumstances should a foreign judgement be recognised and enforced? The first two questions frequently depend on whether the defendant has acted in a manner that justifies the court exercising jurisdiction over her/him and applying the local law to her/his actions. In the Internet context, the assessment of this will often depend on whether the defendant realistically could have avoided coming into contact with the state where the court is located, and geo-identification is crucial in this regard. For example, the possibility, or impossibility, of accurately identifying the geographical location of those who visit a person's website affects what the law reasonably can expect of that person. If, on the one hand, that person can prevent people from particular locations from accessing the website, it could be argued that, by not doing so, she/he has voluntarily accepted the legal risks associated with those people accessing the website. If, on the other hand, that person cannot possibly prevent people from particular locations from accessing the website (without taking it off the Internet and thereby preventing all people from accessing it), it may be much more difficult to argue that such an assumption of risks has occurred.

Both the banking and the securities industries are heavily regulated and providers of services within these fields require licences to be lawful. Where providers of such services make their services available online, they face the problems of the Internet's borderless nature - once uploaded on a website, material is available virtually everywhere in the world. Geo-identification may give providers of services within the mentioned, and other heavily regulated fields, the opportunity to restrict their activities to the areas they are licensed to work within even when making their services available online.

It is interesting to note how some statutes are drafted in a manner suggesting that the legislator is expecting website operators to apply some form of geo-identification. For example, Section 6(1) of the Australian *Interactive Gambling Act 2001* (Cth) states that: "For the purposes of this Act, a prohibited Internet gambling service is a gambling service, where: […] and (c) an individual who is physically present in Australia is capable of becoming a customer of the service." This provision requires website operators to be able to identify the geographical location of those who visit its' websites.

There is a range of aspects of intellectual property law that are affected by and affecting geo-identification. For example, if companies can use geo-identification to know the location of those who visit their websites, they can more easily avoid infringing foreign trademarks, and can avoid violating geographically restricted license agreements. In addition, if geo-location technologies amount to "technological protection measures" under s. 10(1) of the *Copyright Act 1968* (Cth), then the provision of means for circumventing such technologies may amount to a breach of s. 116A of the *Copyright Act 1968* (Cth), thereby making such circumvention unlawful (which would have several serious implication, perhaps particularity in relation to the privacy of those who surf the web).

Privacy law affects and is affected by geo-identification, for example, by the fact that the most common, and most sophisticated, form of geo-identification is based on the translation of Internet Protocol addresses (IP addresses) into geographical locations. Such a technical arrangement require databases of IP addresses to be built, and if it was held that IP addresses constitute personal information under the *Privacy Act 1988* (Cth), those databases may be unlawful.

Taxation is so far one of the few areas in relation to which geo-identification has been discussed in some depth. The question of how best to tax eCommerce has gained considerable attention, and in that context, the Information Technology Association Of America (ITAA) has discussed the potential role of geo-identification.[xvii] Where countries, or groups of countries, seek to impose consumption tax (e.g. VAT) based on the residence of the consumer, the eCommerce businesses need to know the residence of its customers. Geo-identification can help with this, as long as the customer is located at its place of residence at the time of accessing the eCommerce website. However, as noted by the ITAA, current forms of geo-location technologies may suffer from too many weaknesses to be useful for taxation purposes.

Extraterritorial application of a country's criminal or other public law is always controversial. The most studied case of such application, in the Internet context, is *LICRA and UEJF v Yahoo! Inc.*[xviii]. There a French court, 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 (prohibited under the French Penal Code) in dispute. Thus, the perceived existence of feasible technical solutions was determinative. As is clear from, for example, the extraterritorial scope of the *Spam Act 2003* (Cth) and the *Trade Practices Act 1974* (Cth), and cases such as *ACCC v. Chen*[xix], Australia has clearly opted for wide extraterritorial application of aspects of its public/criminal law. The possibility of geo-identification may support this, arguably aggressive, approach.

Australian courts have recently decided two significant Internet defamation disputes. In *Dow Jones v Gutnick*[xx], the High Court ruled that a Victorian court was allowed to exercise jurisdiction over, and apply its laws to, a foreign publisher if the defamatory material published was read by somebody within the state of Victoria. Where the law places such a strong focus on the place of downloading (i.e. where the receiver is located), it clearly becomes extremely important for web publishers to know from where people are visiting their websites. The other relevant case discussed geo-identification specifically. In *Macquarie Bank v Berg*[xxi], the plaintiffs were seeking an injunction restraining the defendant from publishing allegedly defamatory material on a particular website. Having noted how 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, the court refused to grant an injunction. The judge may have come to a different conclusion, had the plaintiffs' legal representatives had knowledge of methods of geo-identification (that existed already at the time of the case).

One of the many issues in contract law, in the context of eCommerce, is the validity of website operators’ attempts to exclude liability by stating that a particular website should not be accessed by people from certain locations. Geo-identification may have several implications in relation to this.

The mentioned areas of law affect virtually all aspects of society, which means that geo-identification also affect virtually all aspects of society.

What is the downside of geo-identification?

The above has demonstrated that the benefits flowing from a website operator being able to identity the geographical location of those who visit its website are undeniable and plentiful. For example, businesses are able to provide targeted advertisement, the risk of fraud can be minimised, and limits may be imposed on the geographical spread of the website’s content. Indeed, as was also demonstrated, in certain areas (e.g. gambling, banking and the securities industry), the law forces website operators to limit the geographical spread of its content.

Yet, it is this limitation that is the greatest concern with geo-identification technologies. Once widely adopted, these technologies will transform the Internet from a borderless medium to something that much more resembles our "real" physical world with all its borders, and at that time the Internet will lose one of its greatest attributes – the "borderlessness".

It is of fundamental importance that regulators are aware of, and take account of, the effect that geo-identification will have on the future structure of the Internet.

Concluding remarks

This article has sought to highlight the dramatic effect that the practise of identifying the geographical location of website visitors will have on the law. From a practitioners' perspective, geo-location technologies highlights the increasing need for lawyers to be technology-savvy. Indeed, the practising lawyers are faced with the daunting task of staying on top of technological development, such as geo-identification. Failure to do so may have devastating consequences.

[*] This article is partly based on Dan Svantesson, *Geo-location technologies and other means of placing borders on the 'borderless' Internet*, John Marshall Journal of Computer & Information Law, Vol XXIII, No 1, Fall 2004; pp. 101 – 139, and Dan Svantesson, *The Impact of Geo-location Technologies on Internet Licensing - Let the Cat and Mouse Game Begin*, Intellectual Property Forum, Issue 63 (December 2005); pp. 24 – 30. Further information about this topic can be found in Dan Svantesson, *Private International Law and the Internet*, Klüwer Law International (January 2007).

[**] 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, Cyberspace Law and Policy Centre - Contributing Editor, World Legal Information Institute (www.worldlii.org) - National Rapporteur (Australia) Data Protection Research and Policy Group, (The British Institute of International and Comparative Law).

[i] 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*: van Leeuwen, Alex *Geo-targeting on IP Address: Pinpointing Geolocation of Internet Users*, Geo Informatics (July/August, 2001); Olsen, Stefanie *Geographic tracking raises opportunities, fears*, CNET News.com, Nov. 8, 2000; and Spangler, Todd *They Know – Roughly – Where You Live*, eWEEK, Aug. 20, 2001.

[ii] "[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.", *at* http://www.webopedia.com/TERM/U/URL.html (last visited 5 February 2007). For more details, *see e.g.* Chappell, Laura A., Tittel, Ed 2002. *Guide to TCP/IP*. Boston: Thomson Course Technology, 271.

[iii] *See further*: http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci212381,00.html (last visited 5 February 2007).

[iv] The methods of collecting this information are discussed below.

[v] *See e.g.* http://www.quova.com/ (last visited 5 February 2007), http://www.akamai.com/ (last visited 5 February 2007), and http://www.digitalenvoy.net/ (last visited 5 February 2007). *See also* the following geo-location products that can be tested for free online: http://www.activetarget.com/livedemo.asp (last visited 5 February 2007), http://www.ip2location.com/free.asp (last visited 5 February 2007) and http://www.geobytes.com/IpLocator.htm (last visited 5 February 2007).

[vi] Digital Envoy product sheet (on file with the author).

[vii] Information Technology Association of America, *ECommerce Taxation and the Limitations of Geolocation Tools*, *at* http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf (last visited 5 February 2007), at 6.

[viii] I.e. Réseaux IP Européens Network Coordination Centre (http://www.ripe.net (last visited 5 February 2007)), American Registry for Internet Numbers (http://www.arin.net (last visited 5 February 2007)), Asia Pacific Network Information Centre (http://www.apnic.net (last visited 5 February 2007))

and Latin American and Caribbean IP address Regional Registry (http://lacnic.net (last visited 5 February 2007)).

[ix] *See e.g. Internet Geography Guide – A NetGeo White Paper* (can be requested from: http://www.netgeo.com/ (last visited 5 February 2007)).

[x] Edelman, Benjamin *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users, at* http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (last visited 5 February 2007), at 3-7.

[xi] Edelman, Benjamin *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users, at* http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (last visited 5 February 2007), at 10.

[xii] Edelman, Benjamin *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users, at* http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (last visited 5 February 2007), at 8. For some examples of anonymising services, *see e.g.*: EPIC Online Guide to Practical Privacy Tools (http://www.epic.org/privacy/tools.html (last visited 5 February 2007)).

[xiii] Edelman, Benjamin *Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users, at* http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (last visited 5 February 2007), at 9.

[xiv] http://www.the-cloak.com/login.html (last visited 5 February 2007).

[xv] http://anonymouse.org/anonwww_de.html (last visited 5 February 2007).

[xvi] See e.g. http://www.quova.com/page.php?id=43 (last visited 5 February 2007).

[xvii] Information Technology Association of America, *ECommerce Taxation and the Limitations of Geolocation Tools, at* http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf (last visited 5 February 2007).

[xviii] *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.

[xix] [2003] FCA 897.

[xx] [2002] HCA 56.

[xxi] [1999] NSWSC 526.