

July 2006

The not so 'borderless' internet: Does it still give rise to private international law issues?

Dan Jerker B. Svantesson

Bond University, dan_svantesson@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation

Dan Jerker B. Svantesson. (2006) "The not so 'borderless' internet: Does it still give rise to private international law issues?". Jul. 2006.

http://epublications.bond.edu.au/law_pubs/96

**Australasian Law Teachers Association - ALTA
2006 Refereed Conference Papers**



**Australasian Law Teachers Association – ALTA
Annual Conference**

61st Annual ALTA Conference

Victoria University, Melbourne, Victoria, Australia
4 – 7 July 2006

Legal Knowledge: Learning, Communicating and Doing

Published Conference Papers

This paper was presented at the 2006 ALTA Conference in the
'International Law' Interest Group

**Australasian Law Teachers Association - ALTA
2006 Refereed Conference Papers**

The Australasian Law Teachers Association (ALTA) is a professional body which represents the interests of law teachers in Australia, New Zealand, Papua New Guinea and the Pacific Islands.

Its overall focus is to promote excellence in legal academic teaching and research with particular emphasis on supporting early career academics, throughout Australasia, in the areas of:

- (a) Legal research and scholarship;
- (b) Curriculum refinements and pedagogical improvements in view of national and international developments, including law reform;
- (c) Government policies and practices that relate to legal education and research;
- (d) Professional development opportunities for legal academics;
- (e) Professional legal education and practices programs.

*Conference Papers published by the ALTA Secretariat
2006*

Edited by Professor Michael Adams, Professor David Barker AM and Ms Samantha McGolrick
Associate Editor Janet Fox

ALTA Secretariat
PO Box 222
Lindfield NSW 2070
AUSTRALIA
Tel: +61 (2) 9514 5414
Fax: +61 (2) 9514 5175
admin@alta.edu.au
www.alta.edu.au

**THE NOT SO 'BORDERLESS' INTERNET:
DOES IT STILL GIVE RISE TO PRIVATE INTERNATIONAL
LAW ISSUES?***

DAN JERKER B. SVANTESSON**

* This paper is partly based upon Dan Svantesson, 'Geo-location technologies and other means of placing borders on the "borderless" Internet', *John Marshall Journal of Computer & Information Law*, (Fall 2004) XXIII (1); Dan Svantesson, 'The characteristics making Internet communication challenge traditional models of regulation - What every international jurist should know about the Internet' (2005) 13(1) *International Journal of Law and Information Technology*.

** (Dr) Assistant Professor, Faculty of Law, Bond University, Australia.

Since its 'birth' approximately 15 years ago, the World Wide Web (WWW) has been viewed as borderless, and this 'borderlessness' has been seen as a major problem in relation to the application of private international law rules to WWW activities. However, recent technological advances let operators of Internet facilities identify the geographical location of those they interact with, enabling them to make their content available in certain locations only. These geo-location technologies can be seen to solve many of the legal problems associated with the Internet's borderlessness.

Having outlined what features of the WWW make it borderless, having noted how current rules of private international law are 'effect-focused', and having discussed the technologies potentially eliminating this borderlessness, the paper examines the extent to which the Internet (particularly the WWW) still give rise to private international law issues.

I RELEVANT FEATURES OF THE WORLD WIDE WEB

While focus often is placed on the Internet's so-called 'borderlessness', a careful analyses shows that WWW communication is associated with several different characteristics that cause what generally is referred to as 'borderlessness'. There are primarily five such characteristics:

Lack of border control: Generally speaking, no controls are carried out when Internet content is transferred across national borders. Thus, for example, it would be difficult for Australia to prevent anti-democratic materials from entering Australia. Such content could be made illegal, but actually preventing it from crossing the borders into Australia would be difficult or impossible. This is due to the Internet architecture in Australia; there simply are no effective strangle-points at the borders.

In contrast, for example the government of the People's Republic of China has rather successfully managed to keep a vibrant Internet usage, while at the same time keeping the level of 'undesirable' content entering the PRC at a minimum. This is due to the fact that Internet content crossing the borders to or from the PRC go via

governmentally controlled gateways.

So to conclude, while some states can control what Internet content crosses their borders, most states do not do so.

Geographical independence: For the average user, there is no clear relation between accessibility of content and the geographical location of content; one can just as easily access a website located on a server on the other side of the planet, as one that is located on a server in the office next-door. Further, the price of Internet communication is relatively independent of distance.

Portability: Internet content may be located on a server in Brasilia one day and in Cairo the next. Further, one and the same website might be mirrored on (eg exist on and be accessed from) any number of servers located anywhere in the world. In addition, a particular website might have its text located on a server located in New Zealand while the pictures are stored on a server located in Zimbabwe.

When the average 'web surfer' accesses a website, he/she ordinarily have little interest in knowing the location of the server(s) carrying the information, and even if he/she wanted to know where the server carrying the website is geographically located, he/she may not be able to find such information. This 'portability', which makes Internet communication significantly different to other forms of communication, is due to the fact that a domain name can be associated with any number of, and varying, Internet Protocol (IP) addresses.

Lack of reliable geographical identifiers: In contrast to other forms of communication, Internet communication lacks reliable geographical identifiers. In WWW communications the only information available is often the IP address, and a domain name. Some domain names contain geographical identifiers, like for example, the website of Bond University¹ In this example, the top-level domain '.au', indicates

¹ <<http://www.bond.edu.au>> at 13 February 2007.

that this is an Australian website. However, this is not what could be classed as a reliable geographical identifier as it is not uncommon for websites of one country to be using the country-code of another country. For example, it is common for Swedish websites to use the country code '.nu' of Niue as *nu* means *now* in Swedish. In addition, a great number of domain names of, mainly but not at all exclusively US, websites do not contain any geographical identifiers, and instead have generic top-level domains such as '.com', '.org' and '.gov'.

Furthermore, while (as is discussed below) there are increasingly accurate technical means for connecting an IP address with a physical location, IP addresses as such, cannot be viewed as reliable geographical identifiers.

Lack of central control: Finally, there is no single or central authority controlling the Internet and Internet communication.² Instead the Internet, in its very structure and architecture, is decentralised. This is, however, not a characteristic unique to Internet communication. There are, for example, no international authorities that can effectively regulate what content may be sent by postal mail or what issues may be discussed on the telephone. In fact, it could be said that private international law rules have never operated in a climate where a single international authority sets the standards. Thus, although the lack of central control is a relevant characteristic of Internet communication, it alone does not make the Internet unique.

It is the combination of these five characteristics that have caused learned commentators to make statements such as that:

Governments cannot stop electronic communications coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that

² The central role of the Internet Corporation For Assigned Names and Numbers (ICANN) in relation to domain names should, however, be noted.

travel electronically to many different nations; one nation's legal institutions should not, therefore, monopolize rule-making for the entire Net.³

II CURRENT RULES OF PRIVATE INTERNATIONAL LAW ARE 'EFFECT-FOCUSED'

The need for website operators to take active steps to regulate their legal exposure is obvious when the current rules of private international law are considered. As is exemplified by the High Court of Australia's judgment in *Dow Jones & Company Inc v Gutnick*⁴, many states will, for example, exercise jurisdiction over, and apply its laws to, a foreign publisher if 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* case⁵, the Canadian *Bangoura* case⁶ and the *Investasia* case⁷ from Hong Kong SAR.

We can, thus, speak of the rules in questions being focused on the location of the effect of the relevant conduct rather than on the location of the actual conduct. Indeed, in *Dow Jones & Company Inc v Gutnick*⁸, the majority of the High Court of Australia went as far as to say that:

However broad may be the reach of any particular means of communication, those who make information accessible by a particular method do so knowing of the reach that their information may have. In particular, those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction.⁹

³ David Johnson and David Post, 'Law And Borders-The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367, 1390.

⁴ [2002] HCA 56.

⁵ *Harrods Ltd. V Dow Jones & Company Inc.* [2003] EWHC 1162 (QB) ('Harrods').

⁶ *Bangoura v Washington Post* (January 27, 2004), OSCJ 03-CV-247461CM1 ('Bangoura') - (Subsequently overruled).

⁷ *Investasia Ltd and Another v Kodansha Co Ltd and another* HKCFI 499 (18 May 1999) ('Investasia').

⁸ Above n 4.

⁹ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56, [39].

This line of reasoning is clearly too simplistic. What the Court is saying is undeniably true, but their observations represents an antiquated view of Internet use, and seems to completely overlook the widespread use of the Internet for domestic, or even local, spread of information. In today's society a website is not only, or indeed always, aimed at attracting distant attention. People rely on the Internet in searching for local information (eg searching for a local restaurant or finding out the opening hours of the local library), and websites are often aimed at a local market. Thus, even if people know that everything they put on the 'net' *can* be accessed from virtually anywhere in the world, that does not necessarily mean that they *intend* to publish in every jurisdiction on the planet, or can *reasonably foresee* publication in every jurisdiction on the planet; knowledge of the sometimes very theoretical potential spread of web-publications does not equate intention to reach a worldwide audience, or indeed, the foreseeability of such spread in the individual case. Unfortunately, the web publishers' intentions and/or foreseeability do not appear to concern the majority of the High Court of Australia.

Furthermore, there are also contract related rules of private international law that are focused on the location of the effect rather than the location of the conduct, and such a focus is, by no means, specific to Australia. For example, the European Union's *Brussels Regulation*¹⁰ contains a provision to the effect that a consumer can only be sued, and can always sue, a business in the consumer's home jurisdiction. Thus, where a dispute arises between a consumer and a business engaged in e-commerce, the court will focus on the location where the business' conduct has an effect, rather than on the location where the business' conduct took place.

Due to the effect-focused rules, the geographical reach of a website operator's legal risk exposure is ordinarily equal to the geographical reach of the website itself. Thus, it is valuable for website operators to be aware of the geographical location of the people who access their website. If a website operator can know the location of those

¹⁰ *Brussels Regulation*, Council Regulation (EC) No 44/2001, of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [Official Journal L 12 of 16.01.2001].

who access the website, he/she can, due to the reactive nature¹¹ of a webserver, 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 website operator with the means to comply with local regulations. Indeed, if there were reliable geographical identifiers, the content provided by a website operator can be adjusted so as to allow the website operator 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 material may be accessible from every state where Internet connection is possible.

III TECHNOLOGIES PLACING BORDERS ON THE ‘BORDERLESS’ INTERNET

Technologies, known as geo-location technologies, are now widely available. There are a number of ways of gaining knowledge of website visitors’ geographical locations. Currently, the most relevant form of geo-location technology is based on the translation of Internet Protocol (IP) addresses into geographical locations, by the use of information stored by the provider of the geo-location service.

When a person enters the appropriate Uniform Resource Locator (‘URL’) 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’ (eg forwards the access-seeker’s IP address) 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. Based on the information in this database, the provider of the

¹¹ A web server’s function is most accurately described as *reactive* (A term, to my knowledge, first used by Roger Clarke in: Roger Clarke, ‘Defamation on the Web: Gutnick v. Dow Jones’, *Baron’s Digest* <<http://www.anu.edu.au/people/Roger.Clarke/II/Gutnick.html>> 13 February 2007. The content of a website 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 (eg the receiver acts and the sender reacts).

geo-location service gives the website server an educated guess as to the access-seeker's location.

There are currently several products on the market utilising this type of system.¹² The technology is not necessarily prohibitively expensive for larger website operators, nor is it particularly difficult to operate.

The accuracy of these products is difficult to gauge. Providers indicate the potential accuracy to be as high as 99 per cent on a country level and approximately 92 per cent on a city-level. However, it should be remembered that they are after all trying to sell a product, and the methods of reaching these impressive figures have been criticised.

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' (eg the problems associated with building up and/or collecting accurate geo-location data) and 'circumvention problems' (eg the problem of people seeking to circumvent the technologies).

Connecting these technologies to what was said above about the Internet's characteristics making it 'borderless', it is clear that geo-location technologies will only affect one of these characteristics; that the lack of reliable geographical identifiers. Yet, while only one out of the mentioned five characteristics changes, the whole dynamic of the problem is changing.

IV ARE THE PRIVATE INTERNATIONAL LAW ISSUES NOW SOLVED?

Since the so-called geo-location technologies discussed above can be said to make it possible for website operators to know, and indeed control, the geographical reach of their Internet content, it could be argued that the effect-focused rules of private international law are now legitimate; as long as the technologies work effectively,

¹² A list of geo-location products, that can be tested for free, can be found on <<http://www.svantesson.org>> at 13 February 2007.

web content can only be accessed by those people the website operator had intended to access it, and thus could foresee accessing it.

This has great benefits. The lack of reliable geographical identifiers meant that there was a diminishing nexus, and sometimes proportionality, between action and effect(s). The effect(s) of an action could occur virtually anywhere, and be totally out of proportion with the action giving rise to it. This resulted in a widening of the reach of effect based jurisdictional rules, which in turn was particularly serious in relation to the extraterritorial application of jurisdictional, and choice of law, rules. For the defendants it lead to a lack of notice, both in relation to where he/she can be sued and even more importantly, which laws he/she had to consider in his/her action. On an international law level, the widening of the reach of effect based jurisdictional rules resulted in a widening of the gap between reasonable grounds for jurisdictional, and application of law, claims on the one hand and reasonable grounds for recognition and enforcement of foreign judgments on the other. Properly functioning geo-location technologies can address these issues.

On the other hand, we must remain alert to the less than perfect accuracy of the mentioned technologies. There can be no doubt that we will still encounter situations where a website operator comes into contact with people from countries the website operator has aimed to avoid, and we must ask how the law should address such situations. There appears to be two alternatives; the law could continue its strict focus on actual contact, or it could focus on whether the website operator had taken reasonable steps to avoid the contact. This latter approach represents the better solution and was anticipated in the previously proposed *Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters*, in which Article 7 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.’¹³

¹³ (emphasis added). *Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters* (June 2001 Draft) art 7.

Furthermore, even if we conclude that it is no longer correct to view Internet communication as being associated with a lack of reliable geographical identifiers, there are still several consequences, of the other four characteristics, that need to be addressed.

First, there is still an imbalance between the ease and cost-effectiveness of entering into Internet-based cross-border contacts on the one hand, and the difficulty and expense of solving cross-border disputes (which can be the result of those contacts), on the other. It cannot be anticipated that private international law rules can address this problem. Instead, efficient and widespread means of Alternative Dispute Resolution must be put into place.

Second, since the Internet, like all other forms of communication, lacks a firm and all-encompassing central control on the international level, individual states have to fill the regulatory function. This results in a situation where decisions are made by individual states. Such decisions may not always be easily recognised and enforced in other states. In other words, the lack of central control means that Internet communication is associated with at least the same degree of recognition and enforcement problems as any other form of cross-border communication. While some states, including Australia, already have in place reasonably flexible rules for recognising and enforcing foreign judgments, other states with little or no such flexibility, such as Sweden, need to accept that globalisation makes necessary effective means for cross-border recognition and enforcement.

Third, even in light of geo-location technologies, some of the grounds used to identify the applicable law, and to determine the appropriateness of jurisdictional claims, in contractual disputes appear, if not directly unsuitable, somewhat far-fetched, artificial and irrelevant in light of the Internet's characteristics. Perhaps the most obvious example is how the location of contract formation is being used as a ground for jurisdiction in many countries including Australia. Learned commentators have

pointed to the flaws of this approach since, at least, 1942¹⁴, and the critique expressed against this approach is even more justified today; not the least, due to the widespread use of the Internet. Any determination of what is the location of contract formation is necessarily artificial when the parties are not in the same forum. While it certainly make sense to say that a contract is formed where the last act necessary to make the contract binding occurred (eg where the offeror receives the acceptance) since only then is the contract actually concluded, one still must question why this should decide the jurisdictional and choice of law questions? What is it that makes that place the proper focal point? One can picture a situation where two parties are exchanging offers and counter-offers only to come to agreement after several rounds of counter-offers. In such a situation it would seem that the place of formation, and thereby the jurisdictional and choice of law questions are determined rather by coincidence. Indeed, in light of the Internet's characteristics it may not even be practical for the parties to ascertain the location of the party they contract with.

V CONCLUDING REMARKS

In light of the above, it could be concluded that the question of whether the Internet in general, and the WWW in particular, will continue to give rise to private international law issues depends on what exactly we mean by 'give rise to private international law issues'. It is clear that the possibility of geo-identification can justify the application of the existing wide jurisdictional rules, thereby in a sense, removing many of the problems associated with the 'borderless' Internet. This is of great significance and will doubtlessly contribute in the determination of the future direction of Internet regulation. However, on the other hand, even with means for geo-identification in place, the Internet in general, and the WWW in particular, will continue to create private international law issues as outlined above.

¹⁴ Robert Neuner, 'Policy Considerations in the Conflict of laws' (1942) XX (6) *The Canadian Bar Review* 498.