

Faculty of Law

Law papers

Bond University

Year 2005

Geo-identification: – Now They Know
Where You Live

Dan Jerker B. Svantesson
Bond University, Dan.Svantesson@bond.edu.au

Geo-identification: – Now They Know Where You Live

Dr Dan Jerker B. Svantesson

Assistant Professor, Faculty of Law Bond University

This article is based on a longer and more detailed article 'Geo-location technologies and other means of placing borders on the 'borderless' Internet', published in the John Marshall Journal of Computer & Information Law

Imagine if website operators could know where you are located as you access their websites. They could then make sure that the content they provided was tailored to people from your location, and provided in the language spoken where you are located. Well, geo-identification – the practice of identifying the geographical location of those who are active online – is not science fiction. Rather, as we 'surf the net', we are frequently identified by location already today. For example, if you visit www.google.com while in Australia, you are automatically presented with the option of going to Google's Australian website. This handy feature is provided as a result of Google, or rather the geo-location technology employed by Google, making an educated guess as to your location.

What has been discussed so far relate to the positive sides of geo-identification. However, this practice also has very troubling effects on the Internet, and of course, massive privacy implications.

How it works

If you are located in Australia and visit the website of US based TV network, Showtime (www.sho.com), you will be greeted with the following message "We at Showtime Online express our apologies; however, these pages are intended for access only from within the United States". As your web browser sends a request to access the website, it includes amongst other things, your IP number. Showtime's web server passes on your IP number to a provider of a geo-location service, in what can be called a "location request". Having built up a database in which IP numbers are matched to geographical locations, the provider of the geo-location service is able to make an educated guess as to your location. This information is passed on to Showtime in what can be called a "location reply", and armed with this information Showtime can determine whether or not it will allow you to access the website.

Geo-identification in the courts

Geo-identification has played a central role in some court cases. In *Macquarie Bank Limited & Anor v Berg*, the plaintiffs were seeking an injunction restraining the defendant from publishing allegedly defamatory material on a particular website, 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 does not lie within the competence of the publisher to restrict the reach of the publication¹".

There can be no doubt that the perceived lack of means of geo-identification played a central role in the judge's decision not to grant injunctive relief. In contrast, based on the expert evidence provided, Justice Gomez in the *Yahoo! Case*², 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.³ Here, the perceived existence of feasible technical solutions was determinative.

It is submitted that 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.

Geo-identification's implications for privacy

Those who thought they were anonymous while online have been both surprised and disappointed over and over again. Considering the widespread use of technologies such as cookies, those active on the Internet should perhaps have grown accustomed to the fact that what they do online is being, or can be, supervised. Yet, that does not appear to be the case, and there is no lack of studies indicating that people want a higher, not lesser, degree of privacy online.

While merely used to identify the country from which a person is accessing a particular website, geo-location technologies are not particularly privacy intrusive. Indeed, their non-intrusive nature is highlighted in the marketing of these products.⁴ However, as the accuracy rates increase, and these technologies can identify Internet users on a city-level, or even street-level, the privacy concerns grow. Currently, the accuracy of these products is difficult to gauge. However, the providers of geo-location technologies indicate the potential accuracy to be very high. For example, 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"⁵

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 problems associated with collecting accurate geo-location data. In relation to IP addresses, there is no equivalent to the address registers listing physical addresses, or the phone registers listing phone numbers. Consequently, when creating databases of geo-location information, one 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,⁶ network routing information, DNS systems, host name translations, ISP information and Web content.⁷ All of these sources may provide inaccurate information.⁸ The second category, circumvention problems, is probably pretty self-explanatory – there are several methods for people with sufficient motivation⁹ 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 server¹⁰), others are easy enough to be used by virtually anyone (e.g. anonymising techniques¹¹) or even inherent in the system-structure ("tunnelling methods"¹²). 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.

Privacy law's implications for geo-identification

If an IP number is classed as “personal information”, the privacy laws of many states apply to the collection, use and disclosure of the IP number. While the developers of geo-location technologies argue that their products are “non-invasive”¹³ and “privacy safe”¹⁴, 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)*¹⁵ (“EC Directive”).¹⁶ Bygrave identifies three criteria by which the EC Directive determines whether or not information constitutes “personal data”:¹⁷

- “the probability of identification”¹⁸ ;
- “the degree of technical ease with which identification can occur”¹⁹ ; and
- “the amount of time and effort demanded by the identification process”²⁰.

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.²¹

The first criterion consequently does not seem to exclude the possibility that IP addresses, in the context of 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.²² 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 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.”²³ 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.”²⁴ 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.²⁵

Thus, 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-independent 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). Of course, it must also be noted that where the geo-location provider manages to connect

an IP number with a very precise location, the location information alone might constitute personal information.

Concluding remarks

There can be no doubt that geo-identification can lower the level of anonymity afforded to Internet users. At the same time, it seems possible that as soon as the practice of geo-identification becomes so exact as to identify an individual, their use becomes restricted by privacy laws.

Even apart from the privacy issues discussed above, the practice of identifying the geographical location of Internet users has major implications. As these technologies becomes more and more widely used, the Internet will inevitably change from a 'borderless' medium, to a communications medium divided by borders, much like the real world.

Dr Dan Jerker B. Svantesson is Assistant Professor, Faculty of Law Bond University, Gold Coast Queensland; Research Associate, Baker & McKenzie Cyberspace Law and Policy Centre; National Rapportuer (Australia) Data Protection Research and Policy Group, British Institute of International and Comparative Law, and Contributing Editor, World Legal Information Institute (www.worldlii.org)

Dan_Svantesson@bond.edu.au, (www.svantesson.org)

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

[2] 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> (last visit May 25, 2004)).

[3] 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> (last visited May 25, 2004)).

[4] Quova's Technical Overview of GeoPoint, at http://www.quova.com/technology/quova_tech_whitepaper.pdf.

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

[6] I.e. Réseaux IP Européens Network Coordination Centre (<http://www.ripe.net> (last visited May 25, 2004)), American Registry for Internet Numbers (<http://www.arin.net> (last visited May 25, 2004)), Asia Pacific Network Information Centre (<http://www.apnic.net> (last visited May 25, 2004)) and Latin American and Caribbean IP address Regional Registry (<http://lacnic.net> (last visited May 25, 2004)).

[7] See e.g. Internet Geography Guide – A NetGeo White Paper (can be requested from: <http://www.netgeo.com/> (last visited May 25, 2004)).

[8] Benjamin Edelman, 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 May 25, 2004), at 3-7.

[9] As correctly noted by Edelman, the motivation for circumventing geo-location technologies seems to vary in accordance with the value of the content (Benjamin Edelman, 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 May 25, 2004), at 7). 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.

[10] Benjamin Edelman, 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 May 25, 2004), at 10.

[11] Benjamin Edelman, 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 May 25, 2004), 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 May 25, 2004)).

[12] Benjamin Edelman, 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 May 25, 2004), at 9.

[13] Digital Envoy, Press Release, of April 9, 2000 at http://www.digitalenvoy.net/news/press_releases/2000/pr_040900.shtml (last visited August 11, 2004).

[14] Quova's Technical Overview of GeoPoint, at http://www.quova.com/technology/quova_tech_whitepaper.pdf.

[15] Official Journal L 281, 23/11/1995 p. 0031 – 0050.

[16] Lee A. Bygrave, Data Protection Law – Approaching its Rationale, Logic and Limits (The Hague: Kluwer Law International, 2002), at 316.

[17] Lee A. Bygrave, Data Protection Law – Approaching its Rationale, Logic and Limits (The Hague: Kluwer Law International, 2002), at 316-317.

[18] Lee A. Bygrave, Data Protection Law – Approaching its Rationale, Logic and Limits (The Hague: Kluwer Law International, 2002), at 316.

[19] Lee A. Bygrave, Data Protection Law – Approaching its Rationale, Logic and Limits (The Hague: Kluwer Law International, 2002), at 317.

[20] Lee A. Bygrave, *Data Protection Law – Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), at 317.

[21] Lee A. Bygrave, *Data Protection Law – Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), at 317.

[22] Lee A. Bygrave, *Data Protection Law – Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), at 318.

[23] Lee A. Bygrave, *Data Protection Law – Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), at 317.

[24] Lee A. Bygrave, *Data Protection Law – Approaching its Rationale, Logic and Limits* (The Hague: Kluwer Law International, 2002), at 317.

[25] See e.g. *Eastweek Publisher Ltd. and Another v Privacy Commissioner for Personal Data* CACV000331/1999 - [2000] HKCA 137 (28 March 2000), *Christopher Harder v The Proceedings Commissioner* [2000] NZCA 129 (17 July 2000), and *Michael John Durant v Financial Services Authority* [2003] EWCA Civ 1746. 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.