EJLT European Journal of Law and Technology

# Finding jurisdiction to regulate Google and the Internet

Conall O'Reilly [1]

Cite as: O'Reilly C., "Finding jurisdiction to regulate Google and the Internet", European Journal of Law and Technology, Vol. 2, No. 1, 2011.

## 1. Introduction

In the recent case of *Football Dataco v Sportradar* [2] , the High Court determined that questions of online jurisdiction hinge on the location of the web-server at hand. As the Internet exists as 'a world that is both everywhere and nowhere', [3] the first part of this paper aims to demonstrate that the reasoning behind this decision is flawed and that its implications are of great concern. To this end, the irrelevance of server location and the lack of legal protection regarding Google's privacy policy will be used as examples of how such an approach surrenders the rights of millions of UK web-users daily.

The second part of this paper aims to show that a better alternative would be to premise jurisdiction on the effects, as opposed to presence, within a particular forum. This paper aims to overcome the numerous challenges to such an approach by identifying what type of activity *should* fall under the remit of forum states and how such an approach *could* work in a way that promotes the type of Internet that is socially desirable. To this end, the issues of policy, certainty and enforceability will be considered so as to conclude that jurisdiction can and should be asserted with regards to disputes that are commercial in nature. In reaching this conclusion, the paper will show how the privacy concerns of Google could be better tackled, and the extent to which this alternative approach would also apply to other common online scenarios.

## 2. The Current Approach

In *Football Dataco,* the claimants argued that the defendants had infringed their copyright and database rights pursuant to UK law. In response, the defendants argued that no such acts had occurred in the UK and therefore they could not be liable for infringement under UK law. Interpreting the *Brussels Regime* [4] so as to conclude that 'it is necessary for the claimants to show in both cases that there is a good arguable case of *an act in the UK* which infringes those rights', [5] Floyd J sided with the defendants. Due to the location of their web-servers, jurisdiction could not be asserted and Sportradar could not be said to have directly infringed UK law.

In reaching his decision, Floyd J applied the Satellite and Cable Directive [6] to Internet activity. He considered the rule that 'the place where the act of broadcast occurs is where the signals are introduced under the control of the person making the broadcast', [7] and concluded that 'the better view is that the act of making available to the public by online transmission is committed and committed only where the transmission takes place'. [8] It is submitted that this interpretation is at odds with the nature of the Internet itself which allows for the copying and dissemination of information from everywhere, to anywhere. In particular, 'emission theory' cannot be considered reflective of online activity and its application potentially renders the rights of UK citizens, in an online context, completely meaningless.

The transmission of satellite broadcasts necessarily involves a large amount of physical presence. Equipment is large and expensive and would, for example, require planning permission. This is not true of online 'transmissions' as web-hosting can be acquired instantly, for free, and from a web-host based in any country of the world. Emission theory and the varied laws of different jurisdictions potentially combine to 'encourage participants in illicit activities to launch their Internet activities from states that provide a legal safe haven'. [9] Floyd J's response to this is that emission theory nevertheless applies to all wireless broadcasts under the Copyright, Design and Patents Act 1988. [10] This ignores, however, the very basis of the argument. Online activity cannot be seen simply as a 'wireless broadcast'.

Firstly, the reach of satellite broadcasting is not comparable to that of the Internet, both in terms of accessibility and how it can be restricted. Billions of people worldwide can, in theory, access every online 'transmission'. In contrast, a satellite transmission from China, for example, will seldom be received in the UK. Whilst satellite transmissions will sometimes carry across the borders of countries in proximity with one another, this cannot be restricted with any deal of precision. Though this was also once true of the Internet, the development of geolocation technology now allows any web-programmer to determine a user's location from his IP address. [11] This can be used either to restrict access absolutely from certain jurisdictions or to tailor the content of a site in accordance with that jurisdiction.

Secondly, whilst satellite transmissions are broadcasts 'into an uninterrupted chain of communication' [12] Internet 'transmissions' are not simply broadcast and received. Instead, data is uploaded to a server and is actively downloaded. Furthermore, whilst satellite communication is unilateral, online activity is increasingly reciprocal. Web-sites are no longer the static HTML based entities they once were; an amalgam of different programming languages allows web-sites to become more interactive than ever. The result of this is that many web-sites 'enlist resources where the user is located by creating an interaction between a remote web service and the processing resources of the user's computer'. [13] As such, the hardware at both points is often utilised and information is continuously being passed between web-user and web-server. Sometimes this information is arbitrary and passed with the user's knowledge but often it is sensitive and the user is unaware. Premising internet jurisdiction on emission theory thus ignores the greater threats that online activity carries.

In ascertaining jurisdiction by way of comparison to a single, traditional medium, the

bigger picture has been missed. It is precisely because the Internet transcends the physical limits of all other media that it is the social phenomenon that it is. The Internet has far greater reach than satellite broadcasts but this needn't always be the case. As a communicative medium with such reach, it encompasses all facets of society including many of the same risks. By premising jurisdiction primarily on the physical location of the web-server, the current approach creates a legal loophole and risks fostering illicit behaviour. It allows those involved in dubious practice to benefit from the Internet's wide reaching, communicative nature easily to escape responsibility for the local effects of their actions.

One notable beneficiary of this grey area in law is Google. Ranked as 'hostile to privacy' by Privacy International, [14] Google retains user-submitted and personally identifying data for the purposes of behavioural advertising. Whilst such data retention is legally permissible where Google is domiciled, it engages and benefits from this activity in Europe where the stricter requirements of the Data Protection Directive are in force. [15] As a voluntary party to the 'Safe Harbor' principles of privacy, Google claims that its privacy policies are 'drafted to comply with the privacy laws in all the countries where we do business'. [16] The veracity of this claim, however, is doubted by the Article 29 Working Party, an independent European advisory body on data protection and privacy brought into force by the Data Protection Directive. In one of many letters addressed to Google, they state that, 'given the predominant role of the Google search engine in the daily lives of all citizens of the European information society, the apparent lack of focus on privacy in this area is concerning', [17] and that they, 'cannot conclude... [that Google] ...complies with the European data protection directive'. [18] As the offending web-servers cannot be pinpointed with any degree of accuracy, compliance with these concerns, under the current approach, depends on voluntary co-operation on Google's part. Thus, whilst the UK's Information Commissioner can apply the rigours of the Data Protection Act 1998 to infringements committed on UK soil, [19] the current approach allows enterprises like Google to escape liability for their equally harmful online activity.

# 3. An Effects-Based Alternative

In his infamous declaration of the independence of cyberspace, John Perry Barlow proclaimed:

> Governments of the industrial world...You have no sovereignty where we gather... Cyberspace does not lie within your borders... We cannot obtain order by physical coercion... Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. [20]

Analysis of *Football Dataco* shows that Barlow is correct to say that the physical concepts of geography and coercion are not applicable to online matters. Examination of Google, however, provides that self-regulation is a naive hope. In light of this, states should not simply abandon the rights of their citizens in the face of technical difficulty but should depart from these traditional concepts and tackle the problems in a more progressive manner. A better alternative would be for courts to focus not on the location of the infringer but on the effects of these infringements within their jurisdiction.

Given the deficiencies of the current approach, the shift from territorial to personal jurisdiction is required as has been recognised to varying degrees in intra-jurisdictional disputes in both the US and the EU. In the US, courts look for 'minimum contacts' made within a state by a non-resident, [21] and for evidence of conduct that 'purposefully avails itself of the privilege of conducting activities within the forum State.' [22] Similarly, in certain pre-scripted scenarios, [23] to which *Football Dataco* is inapplicable, the *Brussels Regime* looks to the defendant's knowledgeable connection within the forum state in asserting jurisdiction. This shift has been problematic, however, and to push this agenda beyond the legal continuity of EC treaty or the US constitution could grossly exaggerate such difficulties.

The biggest problem in asserting personal jurisdiction is that 'so many activities will have effects far beyond their immediate geographical boundaries', [24] and hence that 'assertions of jurisdiction on this basis will almost inevitably tend toward a system of universal jurisdiction'. [25] Whilst 'the rule of law must take precedence over technological choices in establishing the boundaries that society imposes on noxious online behavior', [26] this principle is not universally applied and substantive law will always differ from state to state. Consequently, 'excessive assertions of authority can unduly inhibit extraterritorial activity beyond the courts' legitimate regulatory authority.' [27] The US case of *Barcelona.com* is an acute example of this. [28] This case involved a dispute over a domain name between two Spanish parties which had already been decided with consideration of Spanish trademark law. The Fourth Circuit Court reversed this decision, ignoring Spanish law to find that 'Barcelona' is 'a purely descriptive geographical term entitled to no trademark protection' under US law. [29] Similarly, in *Yahoo!* [30] a French court asserted jurisdiction and issued an injunction against Yahoo! for the removal of any material that violated domestic hate speech laws. Whilst such speech is illegal in France, it is somewhat better-protected in the US. This decision 'threatens to reduce speech on the Internet to the global lowest common denominator', [31] as if French law can override that of the US then so too can any country's law override the law of any other country. Thus, 'the real problem...is not just the individual unfairness to the Yahoo!'s of the world...but the systemic problem that this creates.' [32]

It has been argued that a solution to this problem lies with the use of geolocation technology. As it could be easily used to tailor content in accordance with different jurisdictions, the failure to do so could be seen as 'an indication of the Web publisher's intention to make the content available'. [33] On this view, it could be said that 'Internet activity is "purposely availing" throughout the Internet whenever content is posted without geolocation filtering'. [34] As such, 'the application of effect-focused conflict of laws rules make sense' as web-masters have the tools at their disposal to avoid the risks of litigation. [35] However, whilst it could apply to issues of content, it could not apply to issues of domain name ownership where the issue is that of access to content and not the content itself.

Furthermore, as the Internet 'stands as a singular accomplishment, providing a novel medium by which anyone with even elementary computing skills may communicate worldwide', [36] the crude requirement of geolocation filtration would do great harm to this social achievement. It would have the effect of requiring web-masters to reduce the reach of their pages to jurisdictions where they are familiar with the law. Such familiarity

would seldom transcend that of their own jurisdiction and therefore the global advantages of the Internet itself would be lost. The Internet may not be quite as borderless as previously thought and thus courts have better means to ensure compliance but this power should not be exercised without regard for the type of Internet that is socially desirable.

Asserting jurisdiction therefore requires a distinction between the roles that the Internet plays in society and to the extent to which each role should be regulated. Such a distinction is provided by Stevens J in the landmark case of *Reno* v *ACLU*:

> The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services. [37]

As both the 'vast library' and the 'sprawling mall' serve very different social purposes, a 'jurisdictional doctrine proceeding from an undifferentiated view of the Internet would risk chilling activity in one of the zones'. [38] It follows then, that as a hub of knowledge and discussion, freedom of expression should be promoted in the informational zone and that as a medium that offers instant global commerce, consumers should be protected in the commercial zone. [39] This policy has already been recognised in online jurisdiction disputes both in the US and the EU but to different extents and with varying degrees of success. The problem is that, rather than directly addressing the chilling nature of an effects-based approach, this merely delimits the extent of such consequences to the commercial zone. Given that society benefits from the 'sprawling mall' just as much as it does from the 'vast library' of the Internet, these consequences must be justifiable in theory and mitigated against in practice.

In the EU, Article 15 of the *Brussels Regulation* allows consumers to sue in the place of performance of consumer contracts. [40] This can be seen as problematic for online entrepreneurs as the increases in litigation and travel could 'significantly increase the costs of establishing new businesses online... and restrain the development of e-commerce in Europe'. [41] However in such contracts, the terms are often stipulated by the vendor without the possibility for negotiation and a vendor is better equipped to handle such risks 'either by insurance or by including it as a normal business expense reflected in the price of the end product'. [42] Thus it is justifiable under the assumption that the consumer is 'economically weaker and less experienced in legal matters than the other party to the contract'. [43]

In the US, *Zippo v Zippo Dot Com,* [44] states that web-sites can be seen as active, passive or interactive and that jurisdiction should be asserted accordingly. Active web-sites are those that seek to do business over the internet and purposefully avail themselves in jurisdictions where they do such business. Passive web-sites are those that do little more than offer information to those who are interested in it and cannot give rise to personal jurisdiction. Interactive websites represent the middle ground between the two, where information is exchanged between web-user and web-host and where the more commercial a website's nature is, the more it can be said to purposefully avail itself in a web-user's jurisdiction. The applicability of such a test extends beyond consumer contracts but its justification is analogous; those seeking to *profit* from online activity should be

more *responsible* for the lawfulness of that activity as 'benefits rarely come without costs'. [45]

Whilst the focus on commercial activity can be justified in principle, the application of such a distinction in practice must balance 'the plaintiff's right to sue without significant difficulty, against the defendant's right to avoid forced travel'. [46] To this end, a clear set of jurisdictional rules are required so that web-masters can reasonably foresee what conduct may invoke the laws or jurisdiction of another state. Without such certainty, vendors, fearful of excessive litigation, would be unable to take the necessary steps to follow the law and would be forced grossly to limit the reach of their trade. Similarly, consumers would not be able to predict under what circumstances their national law would apply and thus could not shop with confidence. Methodological certainty is therefore necessary to prevent the development of e-commerce from being unnecessarily curtailed.

In this regard, the *Brussels Regulation* provides certainty by restricting the scope of its application. Article 15(1)(c) provides that in order for a claimant to sue in his state of domicile, the defendant must have pursued or directed activity in that member state. However, the online applicability of this is considerably narrowed given that 'the mere fact that an Internet site is accessible is not sufficient... [and that] language or currency which a website uses does not constitute a relevant factor'. [47] Furthermore, both the *Brussels Regulation* and the *Rome I Regulation*, [48] allow for defendants to escape questions of jurisdiction or choice of law by including a clause to that effect. Combined with the Electronic Commerce Regulations, [49] consumers will automatically lose their jurisdictional rights when forced to click, 'I Accept'. The widespread and template nature of these terms of services and the non-negotiable nature of such contracts combines to negate the very purpose of consumer protection. This fact is reflected in the lack of case law arising from such contracts. It is submitted that a more teleological approach would be to reverse the definition of 'directed activity' and to limit choice of law/forum clauses to negotiable contracts. In the absence of this, the only certainty that the EU's approach provides is that online consumers will invariably be unprotected.

Whilst the EU's stance can be said to provide certainty - albeit for the wrong reasons - the broader approach of *Zippo* fails to provide any certainty at all. *Zippo* provides that jurisdiction depends on the commerciality of a web-site but provides no clear guidelines as to how this should be determined. If a passive web-site is one that simply seeks to provide information, does it cease to be passive if it returns a profit from advertising? [50] Equally uncertain is the sliding-scale test for interactive commerciality. In the absence of clear guidelines as to how commerciality should be determined, jurisdiction hinges on 'fine factual differences', and 'ultimately and unavoidably decisions depend on the judge hearing the case'. [51]

As the EU's approach is too narrow and the US approach too broad, a compromise between the two must prove a better path. *Zippo* is to be welcomed in that it offers protection beyond contractual matters but its scope needs clarification and refinement. At present, *Zippo* looks for effects within a jurisdiction and then assesses the commercial nature of the offending web-site. A better solution would be to assess effects and commerciality simultaneously. In other words, questions of jurisdiction should hinge on the

commercial nature of the effects themselves as opposed to the web-site in general. [52] This would focus not on arbitrary examination of the ever-changing and complicated nature of hybrid web-sites but on guidelines for commercial conduct, to which vast international bodies of law already exist.

Use of geolocation software, coupled with a stricter test for commercial effects, provides the means by which a web-owner can reasonably be expected to find the relevant law of his chosen business in his chosen jurisdictions of practice. Where the law is uncertain or not to his liking, he can filter his content accordingly. Furthermore, this approach actively targets those who do business in a forum and have a vested interest in maintaining business relations with that forum's web-users. The risk of being blacklisted, temporarily or permanently, is an effective means by which courts can ensure geolocation compliance and/or the payment of compensation. Thus, the physical concepts of geography and coercion need not prevent courts from finding the jurisdiction to promote the type of Internet that society desires.

# 4. Applying The Commercial-Effects Test

A basic formulation of a commercial-effects test could read as follows:

> Where A
>
> 1) has infringed B's jurisdictional law, and
>
> 2) this infringement is inextricably linked to commercial activity on A's behalf, and
>
> 3) reasonable care was not taken in avoiding this infringement,
>
> then a court in B's place of domicile will have power of jurisdiction and choice of law

Limbs 1 to 3 must each be satisfied for the conclusion to be reached. Limb 1 applies to any law in B's place of domicile. Limb 2 requires not that there is direct correlation between financial gain of A and the financial loss of B, but that A's commercial gain flows directly from infringement of the law in the forum state. Reasonable care in this context means that if A has not geographically filtered the content or processes of his site to be compatible with B's law, he will fail limb 3. A will have a defence only if the content in question is automatically or user-generated. He will lose this defence if, once notified of the infringement, he did not act accordingly to remove or filter the content. Fulfilment of limbs 1 to 3 would grant the forum court powers of jurisdiction and law. A good arguable case of infringement would still be necessary and the relative needs of both the claimant and defendant would still be balanced in deciding jurisdiction.

This test could apply, not only to instances of contractual breaches or fraud, but also to consumer privacy violations as well. As will be shown, such an approach could be used to ensure that companies like Google actually comply with the data protection laws of the countries they do business in. Whilst Google claims to comply with such laws already, the

concerns of the Article 29 Working Party could suffice in satisfying limb 1. With regards to limb 2, Google profits from an advertising model which relies on data retention on such a large scale. Limb 2 would therefore be satisfied as there is direct correlation between the infringement and commercial gain. Limb 3 would also be satisfied in that Google could tailor its data protection processes with geolocation technology. In the absence of such filtration, reasonable care would be found not to have been taken.

This would mean that if Google refused to co-operate with an audit by the UK's Information Commissioner then it could face legal action in the UK and under UK law. The same is true of any enterprise that displays such disregard for online privacy or for anyone else who infringes on the rights of others for commercial gain. If a case similar to *Barcelona.com* were to present itself, jurisdiction could not be asserted as there would be no commercial effects within the forum state. *Yahoo!* would also be decided differently in that the simple availability of Nazi memorabilia would not be enough to satisfy limb 2. Even with regards to the sale of an illegal item, a site with user-generated content could also rely on the fact that they were unaware of the content in question. Adherence to this approach would provide more reasonable, certain outcomes and prevent the exercise of exclusive jurisdiction. The pitfall of this, however, is that it could not apply to rights where no commercial gain is required.

The requirement of copyright law, for example, is only that copyrighted material is actually copied. In proving that infringement occurs, the law is indifferent as to whether or not the wrong-doer financially gains from his transgressions. Whilst this test could cover those who do profit from such infringements, as in *Football Dataco*, it is the downloading and sharing of vast amounts of media content, for no commercial gain, that is of most pressing concern for copyright holders worldwide. Similarly, defamation law hinges on the simple act of publishing something which results in the loss of reputation for another. Whilst this test could cover defamatory statements through publications accessible only behind a' pay-wall', it is powerless to prevent the instant, global and insuppressible defamatory publications that the Internet makes possible.

However, universal applicability to such legal standards is not to be expected. Given the immeasurable threats of online activity, sacrifices are necessary in order to regulate the Internet with certainty and to allow the "vast library" of the internet to develop freely. Asserting jurisdiction in commercial disputes can be justified and is easier to enforce. Despite this, there will always be online dangers which will be simply out of reach. Whilst public awareness will always play the most important part in protecting web-users, where infringements can be realistically dealt with, they should be.

# 5. Conclusion

The Internet cannot and should not be fully regulated, but attempts should be made in the few areas in which this is possible. Analysis of *Football Dataco* shows that the current approach is out of touch. By premising jurisdiction on the irrelevant location of the server, it offers offenders, such as Google, an easy escape route from liability. Analysis of the EU and US approach provides that they are too narrow and broad, respectively. A better alternative is to focus on the effects of commercial activity within a forum state. This distinction has the effect of protecting freedom of speech in the informational zone and

protecting consumers in the commercial zone. It would regulate Google's privacy infringements and advertising contracts but not their contributions to the informational zone. It is justified as those seeking to profit from global activity should be more responsible for the global effects of their actions. Multi-national corporations must abide the respective laws of the jurisdictions they operate in. The same, in so far as is reasonable, should apply to online enterprises. In practice, claims on this basis will seldom arise due the trivial nature of most transactions and the inordinate costs of litigation. However, this is not to say the possibility of legal action should be denied outright. Where the alternatives are *de facto* legal immunity or ad-hoc adjudication, a commercial-effects test would be the better approach.

# References

Cases

*International Shoe Co v Washington* 326 US 310 (1945)

*Hanson v Denckla* 357 US 235 (1958)

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

*Zippo v Zippo Dot Com* 952 F. Supp. III9 (W.D. Pa. I997)

*Yahoo!,Inc. v. La Ligue Contre le Racisme et l'Antis'mitisme* 169 F. Supp. 2d 1181 (N.D. Cal. 2001)

*Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona* 330 F.3d 617, Civ. No. 02-1396 (4th Cir. 2003).

*Football Dataco Limited and others v Sportradar GmbH and SportradarAG* [2010] EWHC 2911 (Ch)

Journals/Papers

Anonymous (2004) 'A "Category-Specific" Legislative Approach to the Internet Personal Jurisdiction Problem in U.S. Law'. Harvard Law Review, 17(5), 1617-1638.

Anonymous (1999) 'Recent Developments in the Law: The Law of Cyberspace', Harvard Law Review, 112(7),

Anonymous (2003) 'No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet', Harvard Law Review, 116(6), 1821-1844.

Berman P (2002) 'The Globalization of Jurisdiction', University of Pennsylvania Law Review, 151(2), 311-545.

Davis, C (1999) 'Personal Jurisdiction in On-line Expression Cases: Rejecting Minimum Contacts in Favor of Affirmative Acts', 14th BILETA Conference. Accessed at: http://www.bileta.ac.uk/Document%20Library/1/Personal%20Jurisdiction%20in%20Online%20Expression%20Cases%20%20Rejecting%20Minimum%20Contacts%20in%20Favor%20of%20Affirmative%20Acts.pdf .

Kohl U (2002) 'Eggs, Jurisdiction, and the Internet'. The International and Comparative

Law Quarterly, 51(3), 555-582.

Martinez J.S (2003) 'Towards an International Judicial System', Stanford Law Review, 56(2), 429-529.

Ørenm J.S.T (2003) 'International Jurisdiction over Consumer Contracts in e-Europe', The International and Comparative Law Quarterly, 52(3), 665-695.

Reidenberg J (2005) 'Technology and Internet Jurisdiction', University of Pennsylvania Law Review, 153(6), 1951-1974.

Svantesson D (2004) 'Geo-location technologies and other means of placing borders on the "borderless" Internet', Law papers (2004), Accessed at: http://works.bepress.com/dan_svantesson/13

Stein A (2005) 'Parochialism and Pluralism in Cyberspace', University of Pennsylvania Law Review, 153(6),

Websites - Accessed 27/12/2010

Google privacy policy:

http://www.google.com/intl/en/privacy/faq.html#toc-privacy-laws

Article 29 Working Party letter to Google:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf

Information Commissioner's press release regarding Google street view:

http://www.ico.gov.uk/~/media/documents/pressreleases/2010/google_inc_street_view_press_release_03112010.ashx

Privacy International's online privacy rankings:

http://www.privacyinternational.org/issues/internet/interimrankings.pdf

Barlow J.P (1996) 'A Declaration of the Independence of Cyberspace': https://projects.eff.org/~barlow/Declaration-Final.html

---

[1] Queen's University of Belfast

[2] *Football Dataco Limited and others* v *Sportradar GmbH and Sportradar AG* [2010] EWHC 2911 (Ch).

[3] Barlow J.P `A *Declaration* of the *Independence* of *Cyberspace*', (1996), Accessed at: https://projects.eff.org/~barlow/Declaration-Final.html.

[4] In this case, the Brussels Regulation I (Council Regulation (EC) No 44/2001 [2001] OJ L12/1) and the Lugano Convention on jurisdiction and the enforcement of judgments in civil and commercial matters [1988] OJ L319/9.

[5] supra n.2 at [7].

[6] 93/83/EC.

[7] supra n.2 at [66].

[8] *Ibid* at [74].

[9] Reidenberg J 'Technology and Internet Jurisdiction', University of Pennsylvania Law Review, Vol. 153, No. 6, Symposium: Current Debates in the Conflict of Laws (2005), p. 1958.

[10] As amended by the Copyright and Related Rights Regulations 1996 (SI 1996/2967).

[11] See generally, Sventesson D 'Geo-location technologies and other means of placing borders on the 'borderless' Internet', Law papers (2004), Accessed at: http://works.bepress.com/dan_svantesson/13 .

[12] supra n.2 at 66.

[13] Reidenberg supra n.9 at p.1961.

[14] http://www.privacyinternational.org/issues/internet/interimrankings.pdf p.2.

[15] 95/46/EC.

[16] http://www.google.com/intl/en/privacy/faq.html#toc-privacy-laws .

[17] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_05_26_letter_wp_google.pdf p.2.

[18] *Ibid.*

[19] In relation to the StreetView controversy, the Information Commissioner found that, 'Google UK will be subject to an audit and must sign an undertaking to ensure data protection breaches do not occur again or they will face enforcement action', Aaccesed at: t
http://www.ico.gov.uk/~/media/documents/pressreleases/2010/google_inc_street_view_press_release_03112010.ashx

[20] Barlow supra n.3.

[21] *International Shoe v Washington* 326 US 310 (1945).

[22] *Hanson v Denckla* 357 US 235 (1958).

[23] Such as consumer contracts or employment law.

[24] Berman, P., 'The Globalization of Jurisdiction', University of Pennsylvania Law Review, Vol. 151, No. 2 (2002), p. 319.

[25] *Ibid.*

[26] supra n.9 at p.1969

[27] Stein A 'Parochialism and Pluralism in Cyberspace' , University of Pennsylvania Law Review, Vol. 153, No. 6, (2005), p. 2006.

[28] *Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona,* 330 F.3d 617, Civ. No. 02-1396 (4th Cir. 2003).

[29] Ibid. at 629-630.

[30] *Yahoo!,Inc. v. La Ligue Contre le Racisme et l'Antis'mitisme* , 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

[31] 'Towards an International Judicial System', Jenny S. Martinez, Stanford Law Review, Vol. 56, No. 2 (2003), p. 509.

[32] *Ibid.*

[33] Sventesson supra no.10 at p.137.

[34] Reidenberg supra n.9 at p. 1956.

[35] Sventesson supra no.10 at p.138.

[36] Davis C 'Personal Jurisdiction in On-line Expression Cases: Rejecting Minimum Contacts in Favor of Affirmative Acts', 14th BILETA Conference, (1999), Accessed at: http://www.bileta.ac.uk/Document%20Library/1/Personal%20Jurisdiction%20in%20On-line%20Expression%20Cases%20-%20Rejecting%20Minimum%20Contacts%20in%20Favor%20of%20Affirmative%20Acts.pdf .

[37] 521 U.S. 844 (1997).

[38] A "Category-Specific" Legislative Approach to the Internet Personal Jurisdiction Problem in U.S. Law', Harvard Law Review, Vol. 117, No. 5 (2004), p. 1624.

[39] *Ibid.* at p.1628.

[40] Under Article 5, this is determined by the place where the goods were or should have been delivered or were services were or should have been performed.

[41] Ørenm J.S.T 'International Jurisdiction over Consumer Contracts in e-Europe', International and Comparative Law Quarterly, Vol. 52, No. 3 (2003), p. 665.

[42] *Ibid* at p.669.

[43] SUMMARY - CASE C-89/91, *Shearson Lehman Hutton v TVB Treuhandgesellschaft für Vermögensverwaltung und Beteiligungen mbH*, Accessed at: http://curia.europa.eu/common/recdoc/convention/gemdoc93/pdf/01-Z-en-93.pdf

[44] 952 F. Supp. III9 (W.D. Pa. I997).

[45] 'Recent Developments in the Law: The Law of Cyberspace', Harvard Law Review, Vol.112, No. 7 (1999).

[46] 'No Bad Puns: A Different Approach to the Problem of Personal Jurisdiction and the Internet', Harvard Law Review, Vol. 116, No. 6 ( 2003), p.1824.

[47] As stated by the Council and Commission at the Justice, Home Affairs and Civil Protection Council meeting of 30 November and 1 December 2000.

[48] Rome I Regulation (Council Regulation (EC) No 593/2008 [2008] OJ L177/6).

[49] The Electronic Commerce (EC Directive) Regulations 2002 (SI 2002 No.2013), which sets out the requirements necessary for online contracts to be legally valid.

[50] supra n.46 at p. 1838.

[51] Kohl U 'Eggs, Jurisdiction, and the Internet', Vol. 51, No. 3 (2002), p. 565.

[52] supra n.38 p. 1630.