scripted

Volume 11, Issue 2, September 2014

Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?

Dan Jerker B. Svantesson[*]

Abstract

There is a prominent trend of legal actions being taken against globally active Internet intermediaries. This article discusses the extent to which Internet intermediaries should be required to block or remove third-party content, and places emphasis on the geographical limitations that reasonably may be placed on such blocking/removal.

Where an Internet intermediary is ordered to block or remove certain Internet content, global blocking/removal cannot be the default response to every such order. We need a more measured and more sophisticated approach.

This paper canvasses and analyses three such structures. One option is to delineate the reach of the blocking/removal by reference to country code Top-Level Domains (ccTLDs) – "ccTLD-blocking". For example, where a French court requests that Google blocks/removes content in France, Google may do so in relation to www.google.fr, while the relevant content is unmodified for the rest of the world.

Yet, it is also necessary to look beyond ccTLD-blocking. Geo-location technologies may determine an Internet user's geographical location, for example, by reference to the user's IP address. Such technologies can, of course, be used to delineate the accessibility of Internet content. Indeed, such technologies can be used in various ways to achieve such a result and I will consider both a "strict geo-location blocking" and a more nuanced "country lens" approach.

To prepare ground for that discussion, the article first starts with a few appropriate words about the role Internet intermediaries play and why litigants target Internet intermediaries in the first place.

---

[*] Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council. The author sincerely thanks the two anonymous reviewers for their valuable comments.

DOI: 10.2966/scrip.110214.153

1. Introduction – what is the problem?

There is an increasingly prominent trend of legal actions being taken against globally active Internet intermediaries, such as Google and Facebook. While the details are unique to each such action, several disputes relate to content held, but not produced, by the relevant Internet intermediary.[1] The policy considerations involved in assigning liability, or imposing a duty to block/remove content on Internet intermediaries in such cases are complex. As a result of this complexity, we are yet to see a clear international practice develop. Indeed, the reality seems to be a lack of uniformity, not only between different countries, but also within many domestic legal systems.

This article discusses the extent to which Internet intermediaries should be required to block or remove third-party content, and places emphasis on the geographical limitations that reasonably may be placed on such blocking/removal. I argue that we need to be extremely careful in how such a duty is imposed and delineated. Nevertheless, it must no doubt be accepted that occasions will arise where it is reasonable to ask Internet intermediaries to remove or block certain content. Yet, even with the acceptance of this proposition – which ought to be reasonably uncontroversial – we are still left with the task of delineating the geographical reach of such blocking/removal. Given the globalised world we live in, not least online, this is indeed a key question.

In answering this question, we may be tempted to say that when our courts conclude that certain content is to be blocked or removed, we want that blocking or removal to be global. However, the appeal of such a kneejerk reaction will quickly evaporate upon a soberminded consideration of the real state of things. While many people may prefer Internet intermediaries to exercise global blocking/removal based upon orders from the courts of their countries, they may not necessarily wish for Internet intermediaries to engage in global blocking/removal based on court orders from all other countries in the world – particularly where such court orders stem from restrictive, undemocratic laws with an extraterritorial effect. In the end, such compliance risks leading to Internet intermediaries being forced to take account only of the most restrictive laws from all the countries in the world.[2]

To this we may add, a bit simplified, that the geographical reach of a court's order is typically limited to the territory of the country where that court operates. Practical difficulties of giving court orders extraterritorial reach, combined with notions such as sovereignty, comity and the duty of non-intervention, suggest that the geographical reach of court orders typically should be so limited.[3]

---

[1] Such disputes must be kept separate from legal actions taken against Internet intermediaries for their actions going beyond the direct intermediary role. Having said this, one can of course imagine types of disputes in which drawing a clear line between this type of disputes and disputes based on the role as Internet intermediary is far from easy.

[2] I discuss this aspect in more detail in D Svantesson, "Between a Rock and a Hard Place – an International Law Perspective of the Difficult Position of Globally Active Internet Intermediaries" (2014) 30 *Computer Law & Security Review* 348-356.

[3] These matters are discussed in detail e.g. in D Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses" (2014) 50 *Stanford Journal of International Law* 53-102.

Where a globally active Internet intermediary is subject to a court order requesting the blocking/removal of certain content in a certain country, the question is how that Internet intermediary is to delineate the blocking/removal. A global removal would obviously be the most effective approach. However, up until recently, it has been relatively consistently recognised by courts that global removal is problematic and often excessive. Here we can, for example, consider the reasoning of the Supreme Court of New South Wales (NSWSC) Australia:

> An injunction to restrain defamation in NSW [New South Wales] is designed to ensure compliance with the laws of NSW, and to protect the rights of plaintiffs, as those rights are defined by the law of NSW. Such an injunction is not designed to superimpose the law of NSW relating to defamation on every other state, territory and country of the world. Yet that would be the effect of an order restraining publication on the Internet. It is not to be assumed that the law of defamation in other countries is coextensive with that of NSW, and indeed, one knows that it is not. It may very well be that according to the law of the Bahamas, Tazhakistan [sic], or Mongolia, the defendant has an unfettered right to publish the material. To make an order interfering with such a right would exceed the proper limits of the use of the injunctive power of this court.[4]

Thus, a global removal of content that is only unlawful in some countries, but not others, would arguably infringe the rights of people in those latter countries to access that content. Further, global blocking in such a situation may be seen as a violation of the creator's right to communicate that content in the countries where doing so is lawful.

It is important that we do not overlook these rights just because there may be a duty not to communicate that content in some countries. Elsewhere,[5] I have discussed this in some detail, and it may be useful to repeat part of that discussion here. One often sees the adherence to the harshest rules as a proposed solution to the difficulty of variances in legal standards where more than one standard applies to specific conduct. Such suggestions rely on notions, such as that expressed by Justice Souter, that: "[n]o conflict exists, […] 'where a person subject to regulation by two states can comply with the laws of both.'"[6]

I object to this duties-focused approach. Essentially what Justice Souter and others are saying is that we should only focus on the duties imposed by law. If the duties do not conflict, the laws do not conflict. This is too simplistic a perspective. It completely neglects the importance of the rights that laws provide. Importantly, the correlative relationship between rights and duties we may be accustomed to from a domestic law setting does not necessarily survive when transplanted into a cross-border environment; that is, rights provided under one country's legal system may not necessarily create corresponding duties under other legal systems.

---

[4] *Macquarie Bank Limited & Anor v Berg* [1999] NSWSC 526, at para 14.

[5] See e.g. note 2 above.

[6] W S Dodge, "Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism" (1998) 39 *Harvard International Law Journal* 101, at 136.

I argue that in assessing whether two (or more) laws are in conflict we need to take account of both the duties and the rights those laws provide for. In other words, even where the duties do not clash, the rights of one country may clash with the duties of another country.

The difference can be illustrated by way of an example. Imagine that the laws of state A specifically provide for a right of religious freedom, while the laws of state B specifically impose a duty of adherence to Norse pagan faith. Where a person, for one reason or another, finds herself bound to comply with both the laws of state A and those of state B, there is no conflict in the view of the reasoning put forward by Justice Souter and others – such a person can comply with the law of both states by adhering to Norse pagan faith.

In contrast, from the perspective I advocate here, there is a conflict since the right provided by the law of state A cannot be freely exercised while at the same time complying with the duty imposed by the law of state B (except, of course, by those who voluntarily chose to exercise their right to worship Odin, Thor, Freja etc).

In light of all this, I argue that calls for compliance with the strictest rules, as a solution to the problem of conflicting laws, are misguided.

In this context, it is also relevant to consider the practical implications of the fact that most major Internet intermediaries are based in the United States. One thing seems beyond intelligent dispute: the courts that can control Internet intermediaries can to a great extent control the accessibility of Internet content. This fact alone taints the issue discussed with interesting geo-political considerations and agendas. However, concerning ourselves with those considerations and agendas here is quite simply unmanageable.

In light of the above, the core argument, from which the discussion below flows, is that where an Internet intermediary is ordered to block or remove certain Internet content, the default position must be that ordinarily the blocking/removal should be geographically limited rather than having a global reach. Global blocking/removal cannot be the default response to every court order requiring an Internet intermediary to block/remove certain content in a certain country. We need a more measured and more sophisticated approach.

One option is to seek to delineate the reach of the blocking/removal by reference to country code Top-Level Domains (ccTLDs) – we can call this *"*ccTLD-blocking*"*. For example where a French court request that Google blocks/removes content in France, Google may do so in relation to www.google.fr, while the relevant content is unmodified for the rest of the world.[7] This paper investigates the suitability of such a structure.

Yet, it is also necessary to look beyond ccTLD-blocking. After all, technically advanced Internet intermediaries like Facebook, Yahoo, Google and Twitter have

---

[7] For example Google seems to generally be operating in this manner, at least in relation to ex ante blocking: "But when it comes to political extremism it's not as simple. Different countries have come to different conclusions about how to deal with this issue. In Germany there's a ban on the promotion of Nazism -- so we remove Nazi content on products on Google.de (our domain for German users) products."(R Whetstone, "Free Expression and Controversial Content on the Web" (14 November 2007) available at http://googleblog.blogspot.com/2007/11/free-expression-and-controversial.html) (accessed 25 June 2014).

other weapons in their arsenals that can be used to affect the accessibility of Internet content. Geo-location technologies may determine an Internet user's geographical location, for example, by reference to the user's IP address. Such technologies can, of course, be used to delineate the accessibility of Internet content. Indeed, such technologies can be used in various ways to achieve such a result, and I will consider both a "strict geo-location blocking" and a more nuanced "country lens" approach.

First, however, to prepare ground for that discussion, a few words are appropriate about the role Internet intermediaries play and why Internet intermediaries are targeted by litigants in the first place.

2. The important role played by Internet intermediaries

The important role played by Internet intermediaries, as well as the increasing pressure they are under and the need for a clearer legal landscape, were all recognised and articulated in a series of 2010 Organisation for Economic Co-operation and Development (OECD) documents. One such paper noted that: "[l]imitations of liability for Internet intermediaries have enabled these entities and the wider Internet economy to flourish, and facilitated growth and innovation."[8] And that: "governments should clarify how existing laws apply to different scenarios and provide guidance for Internet intermediaries on their legal obligations."[9]

That same paper also stressed that:

> [g]iven the global nature of the Internet and the cross-border services that Internet intermediaries often provide, an international convergence of approaches for the development of policies involving Internet intermediaries was viewed as essential, to provide effective guidance to the business sector.[10]

Despite efforts such as these, if anything, it seems that the potential liability of Internet intermediaries, and more broadly the role such entities ought to play in the Internet ecosystem, is more perplexing than ever. Yet some things seem to be beyond intelligent dispute. For example, focusing primarily on *ex post* blocking/removal:

- Certain types of content, such as child pornography materials, are indefensible, and Internet intermediaries can, and do, play an important role in the fight against such content;[11]
- Intermediaries have existed in various forms for a long time, such as news papers, radio and TV broadcasters and even libraries. Yet, the role and function of Internet intermediaries is so fundamentally different to other types of intermediaries that they must be approached with fresh eyes free from the contamination of preconceived notions based on comparisons with the roles of other intermediaries; and

---

[8] IGF Background Paper, Workshop 105: "The Role of Internet Intermediaries in Advancing Public Policy Objectives" available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (accessed 16 August 2014) at 3.

[9] *Ibid*, 4.

[10] *Ibid*, 6.

[11] Google, for example, has "a global all-product ban against child pornography". See note 7 above.

- It does not lie in the interest of Internet intermediaries to become arbiters of "good taste" or lawfulness of third-party content in a general sense.[12]

In addition, widespread consensus was reached on the following matters already in the 2010 OECD discussions:

- The fact that Internet intermediaries (may) possess the technical capacity to block/remove content does not, on its own, justify them being asked to exercise that capacity;[13]
- The fact that there are many different types of Internet intermediaries excludes a one-size-fits-all approach;[14]
- There is a correlation between imposing legal liabilities on Internet intermediaries and how such entities deal with their users. Such "liabilities can create two effects: i) encourage intermediaries to restrict speech or engage in self-censorship; or ii) discourage intermediaries from allowing anonymous use of their services";[15] and
- There is a need to distinguish between requiring Internet intermediaries to act ex-ante and requiring them to react ex-post.[16] In fact, a relatively recent United Nations (UN) Human Rights Council Report concludes that, "[t]o avoid infringing the right to freedom of expression and the right to privacy of Internet users, the Special Rapporteur recommends intermediaries to: only implement restrictions to these rights after judicial intervention."[17]

Echoing some of the sentiments already expressed above, the Special Rapporteur in the mentioned UN Report notes that:

> [h]olding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law.[18]

---

[12] "Google is not, and should not become, the arbiter of what does and does not appear on the web. That's for the courts and those elected to government to decide." See note 7 above.

[13] See note 8 above, 4.

[14] *Ibid.*

[15] *Ibid*, 10.

[16] *Ibid*, 3.

[17] United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 (16 May 2011) available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (accessed 25 June 2014), at 14. This view is widely held. See e.g. a recent report by ARTICLE19: "Privatised enforcement mechanisms should be abolished. Hosts should only be required to remove content following an order issued by an independent and impartial court or other adjudicatory body which has determined that the material at issue is unlawful. From the hosts' perspective, orders issued by independent and impartial bodies provide a much greater degree of legal certainty." ARTICLE 19, "Internet intermediaries: Dilemma of Liability" available at http://www.article19.org/data/files/Intermediaries_ENGLISH.pdf (accessed 25 June 2014).

[18] United Nations Human Rights Council, note 17 above, 12.

Furthermore, the 24 April 2014 *NETmundial Multistakeholder Statement* also recognises the important role played by Internet intermediaries:

> Intermediary liability limitations should be implemented in a way that respects and promotes economic growth, innovation, creativity and free flow of information. In this regard, cooperation among all stakeholders should be encouraged to address and deter illegal activity, consistent with fair process.[19]

Through this stocktake-like exercise, it is clear that relatively consistent contours of an internationally recognised legal framework for Internet intermediaries are discernible. However, I hasten to add that, as in the case of many other issues, the UN declarations and OECD reports do not reflect actual state practice. They often shine the light onto a desirable path forward rather than onto the less attractive place we are now. For example, the vast gap between e.g. European and Asian approaches to Internet intermediary liability clearly show that the international community is far from reaching a practical compromise on the issue.

3. Why Internet intermediaries are targeted

Given that they are not the primary party responsible for the availability of content, one may wonder why Internet intermediaries are so often targeted instead of the original content providers. The answer to this question may obviously vary from case to case, but without stretching the bounds of imagination too far, it is possible to point to four typical reasons.

First, in many cases, identifying the uploader of the content in question – i.e. the party primarily responsible for its presence online – may be difficult. At any rate, it is almost always considerably easier to identify the provider of the platform on which the content exists (as in the case of e.g. Facebook and Youtube), or from which it can be found and accessed (such as various search engines). In addition, even where an offended party is seeking to take action against the party primarily responsible for the content, it may require the assistance of the relevant Internet intermediary regardless in order to identify that party.

Second, and related to the first, even where the original publisher may be identified, Internet intermediaries may be targeted where the original publisher is beyond the reach of the court where the plaintiff has chosen to take action.

Third, one of the great advantages of digital content is the ease with which it may be copied and re-distributed. This characteristic that generally is a virtue is also a sin where one is seeking to ensure the removal of content from the Internet. One leading commentator goes as far as to argue that "the involvement of intermediaries in the regulatory process signals the beginning of relatively effective law and order on the Internet and ultimately its absorption within the ordinary law of the land."[20]

Finally, Internet intermediaries will typically have "deeper pockets" than do those parties who upload content online (often individuals). This may lead plaintiffs to

---

[19] NETmundial Multistakeholder Statement (24 April 2014) available at http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf (accessed 25 June 2014).

[20] U Kohl, "Google: the Rise and Rise of Online Intermediaries in the Governance of the Internet and Beyond (Part 2)" (2013) 21 *International Journal of Law and Information Technology* 187-234, 188.

include the relevant Internet intermediary in any action they take against the party that uploaded the content. And it may cause plaintiffs to seek large amounts in the litigation.

4. ccTLD-blocking

Country code Top-Level Domains provide a natural geographical delineation of the Internet. Indeed, the idea that the choice of ccTLD is of legal significance is well established. For example, in the combined cases *Pammer v Reederei Karl Schlüter GmbH & KG* and *Hotel Alpenhof GesmbH v Oliver Heller*,[21] the Court of Justice of the European Union stated that the "use of a top-level domain name other than that of the Member State in which the trader is established, for example '.de', or use of neutral top-level domain names such as '.com' or '.eu'"[22] amounts to evidence that the trader's activity is directed to the Member State of the consumer's domicile. In the same case, the Advocate General discussed the matter in detail and states amongst other things that:

> the mention of the internet domain name of a Member State is a clear indication that the undertaking is directing its activities to the Member State with that domain name. If the undertaking – such as Internationale Frachtschiffreisen Pfeiffer in *Pammer*, for example – sets up a website with the domain name '.de', this must necessarily mean that it is directing its activities to the German market.[23]

Elsewhere,[24] I have expressed criticism of some of the reasoning here. In particular, the Advocate General conclusion that: "[i]f, for example, an undertaking with its place of establishment in the United Kingdom sets up a website with the domain name '.es', it is apparent that it is directing its activities in whole or in part to the Spanish market"[25] is of course easily refuted by reference to examples of domain names such as "parti.es" and "famili.es" – domain names that utilise the ccTLD, not for its connection with a particular country, but for its ability to form part of a word or phrase.

Similarly, the geographical delineation provided by ccTLDs is affected by the practice of adopting a ccTLD for its specific meaning. It is, for example, common to see Swedish websites use the ccTLD of Niue (.nu) since "nu" means "now" in Swedish. Another similar example is the prevalent use of Tuvalu's ".tv" for television shows and station with no connection to Tuvalu.

In light of the above, the first thing to note when discussing the reasonableness of blocking/removal within a relevant ccTLD is that not all websites, or indeed all Internet intermediaries, operate with distinct markets delineated by reference to

---

[21] (Case C-585/08) and (Case C-144/09), respectively.

[22] Joined Cases C 585/08 and C 144/09, at para 83.

[23] Opinion of Advocate General Trstenjak delivered on 18 May 2010, at paras 84.

[24] D Svantesson, "*Pammer* and *Hotel Alpenhof* – ECJ Decision Creates Further Uncertainty about when E-Businesses 'Direct Activities' To a Consumer's State under the *Brussels I Regulation"* (2011) 27 *Computer Law & Security Review* 298-304.

[25] Opinion of Advocate General Trstenjak delivered on 18 May 2010, at para 85.

ccTLDs. Consequently, ccTLD-blocking is only of relevance for those major – typically globally active – Internet intermediaries that have adopted a ccTLD-based structure. For example, Google operates country-specific websites differentiated by different ccTLDs. Thus, users in Sweden would typically access google.se while users in the UK would visit google.co.uk.

Nevertheless, in many cases the reliance on ccTLDs as delineating online markets is justified. After all, if a company's choice of ccTLD can be seen to indicate its intention to target a particular market in the context of a jurisdictional analysis (as in the mentioned *Pammer/Hotel Alpenhof* case), that same choice must reasonably be seen as of importance also in relation to the delineation of court order-based content blocking.

Importantly in its context, the Advocate General also stated that "the use of a Member State's internet domain name does not preclude the directing of activities to other Member States." However, for our discussion here, that matters little given that it would be hard to argue that e.g. google.se is directed at the Danish market as such when there is also a google.dk site.

The conclusion must be that, if approached with care and with an awareness of its limitations, ccTLD-blocking is one possible tool to delineate the geographical reach of court order-based content blocking by certain types of globally active Internet intermediaries.

5. Geo-location technologies[26]

Over the past ten years, I have written fifteen articles and notes, and given numerous talks and conference presentations, on the legal implications of geo-location technologies. Perhaps the fact that I still get to publish on this topic can be viewed as a testament to the limited impact my writings and other activities in this field have had to date. However, geo-location technologies remain of significant legal importance.[27] And while the law, and law makers, slowly are becoming aware of these technologies,[28] members of the Internet industry are already avid users.

---

[26] In parts, this section draws, and expands, upon previous publications on related topics such as: D Svantesson, *Private International Law and the Internet 2nd ed* (Alphen aan den Rijn, Netherlands: Kluwer Law International, 2012), and D Svantesson, "Time for the Law to Take Internet Geo-location Technologies Seriously" (2012) 8 *Journal of Private International Law* 473-487.

[27] See e.g. N Selvadurai, "The Proper Basis for Exercising Jurisdiction in Internet Disputes: Strengthening State Boundaries or Moving towards Unification?" (2013) 13 *Pittsburgh Journal of Technology Law and Policy*; M Trimble, "The Future of Cybertravel: Legal Implications of the Evasion of Geolocation" (2012) 22 *Fordham Intellectual Property, Media and Entertainment Law Journal* ; K F King, "Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies" (2011) 21 *Albany Law Journal of Science and Technology* 61; M Fagin, "Regulating Speech across Borders: Technology vs. Values" (2003) 9 *Michigan Telecommunications and Technology Law Review* 395; J Burnett, "Geographically Restricted Streaming Content and Evasion of Geolocation: The Applicability of the Copyright Anticircumvention Rules" (2012) 19 *Michigan Telecommunications and Technology Law Review* 461; J R Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1998) 76 *Texas Law Review* 553; M Geist, "Is There a There There? Towards Greater Certainty for Internet Jurisdiction" (2001) 16 *Berkeley Technology Law Journal* and D Svantesson, "Geo-Location

Geolocation services and location-aware software applications have become increasingly popular over the last decade both online and on mobile phones. They cover a vast array of services that include mapping and navigation (such as Google Maps and Ovi by Nokia), social networking (such Facebook and Foursquare) and security for lost or stolen mobile phones (such as HTCSense.com). Such services can tell users (and if they wish, others) where they are and allow them to receive content relevant to their location without having to manually enter the address or postcode. Such are the benefits and convenience of geolocation services and location-aware applications. They are quickly becoming an essential and expected aspect of being online for many users.[29]

These technological advancements are in large part motivated by perceived business advantages. For example, if a website operator can see where access-seekers are located, "geographically appropriate" advertisements can be specifically targeted at those individuals. Other perceived advantages include, for example, ensuring regulatory compliance, spam minimisation, reducing fraud risk and keeping licensed content within geographical boundaries. Finally, introducing location-sensitivity into online services may make them more user-friendly, thereby improving the users' experience.

The providers of geo-location technology services indicate the potential accuracy to be very high. Having surveyed a range of geo-location services, Shavitt and Zilberman note that "[a]ll the databases claim to have 97% accuracy or more at the country level and 80% or more at the city level".[30] Such figures can, of course, always be criticised. First of all, when assessing the accuracy of methods for geo-identification, it is important to avoid placing the focus on the marketing-driven *average* accuracy-rates presented by the companies behind the method in question, and instead pay attention to the *context-specific* accuracy rate.

If a company were to assert that its method is, for example, "98% accurate" on average across all its applications involving analysis of locations throughout the world, it is likely that the accuracy rate for Canadian and American location

---

Technologies and Other Means of Placing Borders on the 'Borderless' Internet'" (2004) XXIII *John Marshall Journal of Computer and Information Law* 101–39.

[28] For example, the existence of geo-location technologies was overlooked in *Pammer v Reederei Karl Schlüter GmbH & KG* and *Hotel Alpenhof GesmbH v Oliver Heller* (Case C-585/08) (Case C-144/09), respectively, and disputed in *Macquarie Bank Limited v Berg* [1999] NSWSC 526. In contrast, and more encouragingly, in the joined cases of *eDate Advertising GmbH v X* (Case C-509/09 (Referring court Bundesgerichtshof, Germany)) and *Olivier Martinez, Robert Martinez v MGN Ltd* (Case C-161/10 (Referring court Tribunal de grande instance de Paris, France)), Advocate General Cruz Villalón pointed to the existence of geo-location technologies. Furthermore, geo-location played an important role in, for example, *International League Against Racism & Anti-Semitism (LICRA) v Yahoo! Inc* [2000] County Court of Paris, and was noted in cases such as: *National Federation of the Blind v Target Corp*, 452 F Supp 2d 946 (N D Cal 2006), *Hageseth v Superior Court*, 2007 Cal Daily Op Service 5647, *ACLU v Gonzales* 478 F Supp 2d 775 (ED Pa 2007), Bavarian Administrative Court BayVGH Judgment of 20 November 2008 10 CS 08.2399, and OVG Thüringen Decision of 3 December 2008 Az 3 EO565/07.

[29] M Watts et al, "Do European Data Protection Laws Apply to the Collection of WiFi Network Data for Use in Geolocation Lookup Services?" (2011) 1 *International Data Privacy Law* 149, 149.

[30] Y Shavitt and N Zilberman, "A Study of Geolocation Databases" (1 July 2010) Cornell University Library available at http://www.epic.org/privacy/tools.html (accessed 25 June 2014), at 3.

distinctions alone is lower than 98%, given the unique difficulties in this context.[31] Placing the focus on context-specific accuracy rates will inevitably complicate and increase the cost of court proceedings in that expert evidence may be required in each individual case. However, the importance of ensuring that the courts base their decisions on the accuracy rate that is relevant in the particular case at hand cannot be overstated.

Second, there is no reason to assume that accuracy rates presented today will hold true in the future. Changes in Internet technology occur with great frequency and may severely impact the accuracy of geo-location technologies.

Third, the accuracy rates mentioned above are based on the assumption that no active steps are taken by the Internet users to circumvent the geo-location technologies used. That assumption quickly loses validity once one steps out of the lab and into the real world. Where content is sufficiently valued by Internet users, they may seek to circumvent the geo-location technologies used in order to access that content. While some circumvention techniques are technologically advanced (e.g. deep linking to streaming video content without accessing the HTTP server[32]), others are easy enough to be used by virtually anyone (e.g. anonymising techniques[33]) or even inherent in the system-structure ("tunnelling methods"[34]). With this in mind, it will presumably always be possible to circumvent geo-location technologies.

Even with the caveats above in mind, the argument can be made that Internet intermediaries ought to supplement, or indeed replace, ccTLD-based blocking/removal with blocking/removal based on the geographical location of the user as identified through geo-location technologies. Where geo-location technologies are used to *prevent Internet users from accessing certain content*, we may speak of "strict geo-location blocking". In contrast, where geo-location technologies are simply used to *guide users to certain content*, we may speak of a "country lens" approach. I will discuss both of these options.

5.1 Strict geo-location blocking

The use of geo-location technologies to prevent Internet users from accessing certain content – strict geo-location blocking – is not free from risks. First of all, as noted above, geo-location technologies may be circumvented, and thus it must always be remembered that there may be leakage.

---

[31] B Edelman, "Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users" available at http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf (accessed 25 June 2014), at 6. The "unique difficulties" Mr Edelman speaks of are multiple. First, a number of Internet service providers (ISPs) offer their services in both the US and Canada. Second, the proximity and economic ties between the two countries mean that many companies have offices in both countries. Third, he notes the widespread use of intranets with a single access point to the Internet. Fourth, communication between Canada and the US is not particularly likely to pass through well-known "peering points" or contain the telltale transoceanic time delays.

[32] *Ibid*, 10.

[33] *Ibid*, 8. For some examples of anonymising services, see e.g.: "EPIC Online Guide to Practical Privacy Tools" available at http://www.epic.org/privacy/tools.html (accessed 25 June 2014).

[34] *Ibid*, 9.

Second, there are obvious privacy implications associated with requiring Internet intermediaries to block content based on the location of their users.[35] The severity of these implications depend, however, on the extent to which the Internet intermediary already relies on linking user location with content access e.g. for advertisement purposes. Obviously, where this is already done, any argument that requiring blocking based on geo-location technologies undermines user privacy is of limited relevance.

Third, and more seriously, consequences of a severe nature are in store if an extensive use of strict geo-location blocking becomes the norm rather than the exception. After all, geo-location technologies have the power to transform the Internet as we know it into something that more closely resembles our "real" world. In doing so, geo-location technology risks destroying one of the Internet's most valuable and unique characteristics – its borderless nature.[36]

Ultimately, whether strict geo-location blocking is desirable or not depends on whether we want the blocking to be as effective as is technically possible, or whether we are prepared to take a more relaxed attitude, perhaps justified by reference to a greater good for the Internet's openness, or perhaps by a fear of other country restricting content.

In any case, both ccTLD-blocking and geo-location technologies can be circumvented. If it is perfect blocking we are looking for, we have to look elsewhere. And I suspect we would always be looking in vain.

5.2 The country lens approach

A possible compromise can be found in the fact that we can use geo-location technologies to guide users to country-specific pages instead of using such technologies to prevent access to foreign content.

We can here see a convergence of geo-location technologies and ccTLD-blocking. When typing in www.google.com while in Australia, one is automatically taken to www.google.com.au when pressing the enter key.[37] Similarly, when typing in www.yahoo.com while in Australia, one is automatically taken to Yahoo's Australian

---

[35] A considerable proportion of recent literature on geo-location is focused on privacy. See e.g.: R Mura, "Geolocation and Targeted Advertising: Making the Case for Heightened Protections to Address Growing Privacy Concerns" (2013) 9 *Buffalo Intellectual Property Law Journal* 77; T J Van Hal, "Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection" (2012-2013) 15 *Vanderbilt Journal of Entertainment & Technology Law* 713; T Claypoole and R C Balough, "Privacy Considerations Limit Geolocation Technologies" (2012) *Business Law Today* 1 and A Diaconescu and C C Basarabescu, "Private Life and Geo-localisation" (2013) *Annals of Constantin Brancusi University of Targu-Jiu: Juridical Science Series* 103. See also: ARTICLE 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices adopted on 16 May 2011 (881/11/EN WP 185).

[36] See further: C O'Reilly, "Finding Jurisdiction to Regulate Google and the Internet" (2011) 2 *European Journal of Law and Technology* and D Svantesson, "Time for the Law to Take Internet Geo-location Technologies Seriously", see note 26 above.

[37] Test performed 27 March 2014. On some occasions in the past, instead of being taken to www.google.com.au, one was taken to www.google.com but with a link conveniently offering a transfer to Google Australia.

website when executing the command.[38] Intermediaries do this for a range of reasons, such as providing country-relevant marketing and content. Perhaps somewhat paradoxically then, the necessity of Internet intermediaries supplementing ccTLD-blocking with geo-location technology based blocking depends, at least in part, on the extent to which such technologies are used more generally to guide users to the "geographically appropriate" ccTLD version of their sites. Arguably, the stricter the control that guides users to the geographically appropriate ccTLD site as default, the less legitimate are calls for strict geo-location blocking.

Importantly, there is, of course, no necessity in linking this type of geo-location use to ccTLD-blocking, and when Internet businesses guide users to a country-specific version of their service, that version can be identified by means other than the traditional ccTLD designation. In other words, some sites provide a country-specific user experience without delineating their content by ccTLDs – a country-specific user experience is provided within the one and same TLD (typically ".com").[39] This type of "country lens" approach has the distinct advantage of avoiding the problems highlighted above in relation to ccTLD-blocking. At the same time, ccTLD delineation may have a transparency advantage in that users always can check the ccTLD to identify which country's content they are being presented with. To cater for a similar degree of transparency where the country lens approach is divorced from ccTLD delineation, the Internet intermediaries may, on the web pages they display, include a prominently displayed icon indicating which country's content the users are being presented with. For example, one could imagine a standardised banner along the left-hand side of the screen clearly indicating the relevant country both in text and in picture, such as the country flag.

Whether one advocates the country lens approach to be tied to the ccTLD system or not, anyone favouring some form of country lens approach must consider the extent to which Internet users should be able to steer away from the country-specific site they are guided to. In her excellent paper "The Future of Cybertravel: Legal Implications of the Evasion of Geolocation", Trimble refers to this as "cybertravel".[40] It is this – the built in unrestricted ability to cybertravel – that sets the "country lens" approach apart from strict geo-location blocking.

This consciously provided option, to disconnect from the particular country-specific user experience the geo-location technologies would otherwise guide the user to, can be catered for in a variety of ways. As technologies advance, we may see new ways to achieve this, but here it suffices to point to two possibilities. For example, the disconnection from the guided path provided by the geo-location technologies may be activated by the users' browser settings. In other words, a structure may be adopted allowing the geo-location technology's selection of country-specific content to be overridden by user selected browser settings. Alternatively, the Internet intermediary may itself provide the tools for users to deviate from the country-specific content the

---

[38] Test performed 27 March 2014.

[39] Consider, for example, Twitter. See further: "Country withheld Content" (2014) available at https://support.twitter.com/articles/20169222-country-withheld-content# (accessed 25 June 2014).

[40] M Trimble, note 27 above, 567.

geo-location technology would have guided them to.[41] The key point here is that there is no need for any technological revolution in order for the country lens approach to work – all necessary technological components already exist, and in fact, they are already being used. All that it takes now is the initiative to clarify the country lens approach's legal status.

By catering for cybertravel, the country lens approach avoids the most severe of the problems with strict geo-location blocking; that is, it avoids the destructive impact on the Internet's "borderlessness" and it avoids over- and under-blocking where geo-location errors occur. Importantly, it does so while still maintaining the key benefit of geo-location technologies – their ability to create a country-specific user experience.

Such an arrangement meets one of the fundamental requirements I have pointed to for some time. Since 2001, I have argued that rather than focusing on whether content was *targeted* at a particular jurisdiction, as is commonly done, we should focus on *"dis-targeting"*[42] – what steps, if any, were taken to avoid contact with the jurisdiction in question? By excluding certain content from the country-specific user experience, an Internet intermediary is actively dis-targeting that excluded content from that particular country. Such an active step should typically ensure that the intermediary is beyond liability for the content in question.

Critics of the country lens approach will no doubt point to the fact that it does not effectively prevent people in a particular country from accessing content a court has ordered be blocked there. Internet users with a sufficiently strong desire will simply access that content through cybertravel. Consider, for example, a search engine that has been ordered to block certain search results. Where the blocking is in the form of the country lens approach, or indeed ccTLD-blocking, it is easy for users to still access the content. In light of this, there may be a temptation to favour strict geo-location blocking. However, first of all, it has already been illustrated that circumventing strict geo-location blocking is not demanding. And, even more importantly, at least in the case of search engines, even the most vigorous opponents of the country lens approach must recognise the availability of alternative search engines. Thus, even if a particular search engine was to have the technical ability to flawlessly block certain search results to the people of a particular country, persons in that country could simply use an alternative search engine to find and access the relevant materials.[43]

Finally, it remains to be noted that, like in the case of strict geo-location blocking, in making necessary the identification of Internet users' locations, the country lens has obvious privacy implications. However, as in the case of strict geo-location blocking, the severity of these implications depend on the extent to which the Internet

---

[41] Consider, for example, Twitter. See further: "Changing Your Country's Settings" (2014) available at https://support.twitter.com/articles/20169220# (accessed 25 June 2014).

[42] See e.g.: D Svantesson, "What Should Article 7 – Consumer Contracts, of the Proposed Hague Convention, Aim to Accomplish in Relation to E-commerce?" (2001) 17 *Computer Law & Security Report* 318-325.

[43] Here we may pause to consider the competition law implications of a court order requiring one search engine to block/remove certain content where that court order does not affect other, competing, search engines.

intermediary already relies on linking user location with content access e.g. for advertisement purposes.

In light of this, it appears that the country lens approach tallies up more virtues and fewer vices than do ccTLD-blocking or strict geo-location blocking.

6. The reasonableness of blocking/removal beyond the country ordering the blocking

All three approaches discussed above have been analysed in the context of being used to provide blocking/removal limited to certain content in a certain country. The extent to which a court order in one country should force Internet intermediaries to block/remove content beyond that country is an even more complex matter taking us deep into the quagmire of public international law, state sovereignty and the duty of non-intervention. Clearly, it is a matter in relation to which we must again recall the mantra that "one-size-does-not-fit-all". And it is a matter involving the same set of considerations regardless of whether the blocking/removal beyond the country ordering the blocking is carried out through ccTLD blocking, strict geo-location blocking or the country lens approach. Indeed, where global blocking/removal is requested, there will of course be no need to base the blocking on either of the three approaches analysed in this article.

In my view, we cannot discuss the reasonableness of blocking/removing beyond the country ordering the blocking in generic terms. Instead, we must adopt a context-specific approach and discuss different legal areas independently. For example, it may be reasonable to expect the blocking/removal of child pornography materials to be carried out globally, i.e. across the entire range of platforms under the control of an Internet intermediary – including across all TLDs. However, that does not necessitate the conclusion that the same level of reaction is justified e.g. in relation to content that is deemed to violate some intellectual property right in the country handing down the court order. Consequently, the extent to which a court order in one country should force Internet intermediaries to block/remove content beyond that country must depend on the type of legal action that produced the relevant court order.

Furthermore, given the special role commonly played by Internet intermediaries, even where it is appropriate to require an original publisher to remove content globally, it may not necessarily be justifiable to require an Internet intermediary to extend its blocking globally. For example, whether Germany ought to issue take down orders, with global effect, against Germans who have uploaded Nazi propaganda is a different matter to whether German courts ought to require Internet intermediaries to block/remove such content globally or only for Germans e.g. through ccTLD blocking, the country lens approach or indeed, through strict geo-location blocking.

Drawing upon the discussion above, I propose the following four broad principles:

Principle 1: *The extent to which a court order in one country should force the blocking/removal of content beyond that country must depend on the type of legal action that produced the relevant court order.*

Principle 2: *Generally, orders requiring global blocking/removal should only be awarded against the party who provided the content, not parties that merely act as intermediaries in relation to that content. And such orders should only be awarded by the courts at the defendant's place of domicile.*

Principle 3: *Exceptions to Principle 2 should be made in relation to particularly serious content such as child pornography materials.*[44]

Principle 4: *In relation to rights limited to the territory of a specific country, whether based on registration or not, courts should not order blocking/removal beyond that country.*

These principles do obviously only cover a selection of issues, and are merely meant as a starting point for further discussion.

7. Concluding remarks

The above has illustrated that global blocking/removal cannot be the default response to every court order requiring an Internet intermediary to block/remove certain content in a certain country. And it was argued that ccTLDs represent a potential tool to delineate the reach of court order-based content blocking/removal by globally active Internet intermediaries. However, it was also highlighted that ccTLD-blocking is associated with certain weaknesses. Thus, the alternative of using geo-location technologies was examined in some detail. It was concluded that what we may call a strict geo-location blocking interferes too much with the aim of a (relatively) borderless Internet. Instead, I proposed a more nuanced country lens approach making use of geo-location technologies to guide Internet users to a country-specific user experience, while at the same time maintaining the option for users to explore Internet content beyond that country-specific user experience.

It was shown that the approach discussed works to avoid situations where attempts at regulating the Internet within one country have a spill-over effect globally. Further, I demonstrated that the extent to which a court order in one country should force the blocking/removal of content beyond that country must depend on the type of legal action that produced the relevant court order.

While hopefully this analysis of ccTLD blocking, strict geo-location blocking and the country lens approach was useful, much has been left unsaid in this short article. For example, no attempt has been made to assess the implementation costs associated with the three different methods. Further, no attempt was made to analyse how the three alternatives sit within any particular state's legal system. The discussion was broader, and in a sense more introductory. Doubtlessly, both these issues deserve detailed attention in future research efforts.

In addition to the analysis of the three different methods discussed, an attempt was made at conducting a stock taking exercise seeking to identify the contours of an internationally recognised, but yet to be adequately implemented, legal framework for Internet intermediaries. In that context, several broad principles were identified that ought to amount to a useful foundation for any future attempt at regulating the liability of Internet intermediaries.

To conclude the discussion, I wish to stress that all the alternatives discussed represent compromises. And like most, if not all compromises, it is unlikely that any

---

[44] Identifying what amounts to such "particularly serious content", and indeed defining "*child pornography materials"*, are interesting and complex tasks, not least given the different attitudes held in different parts of the world. However, embarking on such an exercise would take us too far afield in this brief article.

of the approaches will be viewed as ideal by any party. However, perhaps the country lens approach is the delineations method that can gain the broadest support by the relevant stakeholders (of which the there are many indeed).