UNIVERSITÉ DE GENÈVE

Geneva Internet Disputes Resolution Policies 1.0

www.geneva-internet-disputes.ch

Geneva Internet Disputes Resolution Policies 1.0

Introduction

Background and policy topics covered by the GIDRP 1.0

The Geneva Internet Dispute Resolution Policies 1.0 (GIDRP 1.0) project has emerged as a result of an international conference that took place at the University of Geneva on 17 - 18 June 2015 at which leading experts presented and discussed selected facets of the numerous challenges of Internet-related disputes (www.internet-disputes.ch).

In the months following the conference, a team of researchers from the University of Geneva has taken up the challenging mission to draft detailed policy proposals on pressing issues that can arise in the course of legal disputes relating to the Internet/IT industry. These policy proposals focus on the following four fundamental issues:

- Which national courts shall have jurisdiction in Internet-related disputes (Topic 1)?
- How to structure an alternative dispute resolution system for Internet-related disputes (Topic 2)?
- How shall disputes about the licensing of Standard Essential Patents (SEP) under Fair, Reasonable and Non-Discriminatory (FRAND) terms be solved (Topic 3)?
- How shall immunities apply on the Internet (Topic 4)?

Invitation to comment on GIDRP 1.0 & to participate in GIDRP 2.0

The GIDRP 1.0 obviously does not ambition to offer an ultimate and final solution to the legal issues that it addresses. Its objective is to contribute to the global debate and to facilitate the emergence of global standards that shall ensure efficient and equitable justice in the Internet era.

The GIDRP 1.0 is a digital policy project: it is not carved in stone and is not even materialized in any paper publication. The reason is that the GIDRP 1.0 is conceived as a work in progress (more precisely: a *policy* work in progress), that must be discussed, criticized and improved by a process of broad consultation and inclusive participation.

On this basis, institutions and people are strongly **encouraged to share their comments** on the GIDPR 1.0 by sending an email at GIDRP@unige.ch or by using the comment box on the website and are also invited to participate to the project which will hopefully materialize in the issuance of GIDRP 2.0. Of course, the GIDPR 1.0 can also be endorsed either as a whole or only for specific policy proposals.

* * *

Topic 1

Which national courts shall have jurisdiction in Internet-related disputes?

Introduction

- The emergence of the Internet, a borderless and international medium for communication and commerce, has enabled both physical and legal persons to regularly engage in a wide range of activities having a cross-border element. E-commerce has made it easy for companies and consumers alike to order goods and services from businesses located abroad; similarly, the global availability of websites has furthered the reach of torts, such as defamation, privacy offenses and copyright infringements, allowing them to cause harmful effects in multiple jurisdictions at the same time. This begs the question: when a given online contract or tort gives rise to litigation, which courts have jurisdiction to decide?
- Questions of jurisdiction have been traditionally answered by the application of principles of international private law. For example, it is acknowledged that jurisdiction may be found, as regards contracts, before the courts located at the place of its performance,[1] and, as regards torts, before those located at the place of the harm committed.[2] The Internet, being a common global space in which acts cannot be attached with certainty to a geographical location, has majorly challenged the functioning of these territorially-bound rules. In that sense, some early writings about this issue have suggested that cyberspace, i.e. the "place" of the Internet, should be considered as a separate sovereign space which should be governed by its own judicial and legal system.[3]
- Today, it has come to be accepted that the Internet is subject to the jurisdiction of national courts regarding acts committed there.[4] The current issues are thus more about how to adapt the existing rules of international private law to fit the borderless boundaries of the network; in particular, a common running theme in these discussions concern the required level of contacts that a website should entertain with a particular jurisdiction in order to be fully subject to the jurisdiction of the courts there without causing prejudice to, one the one hand, the principle of foreseeability of the forum, and, on the one hand, and the rights of access to justice.[5]
- The topic has very practical implications. From the point of view of owners of website, jurisdictional rules should be clear enough in order to allow them to expect in which parts of the world are they liable to be sued; from the point of view of users, consumers and tort victims, it is important that they may be able to rely on the jurisdiction of courts that are close to their interests.
- The principles listed below have been developed as a response to challenges raised by various areas of Internet law, however they do not apply equally to all of covered subjects. These are:
    - Business to business contracts (proposal 1).

---

1 See article 7 (1) of Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), *Official Journal of the European Union*, 20.12.12, L 351/1 (hereafter referred to as 'Brussels I Regulation (recast).

2 See *id.,* article 7 (2).

3 David R. Johnson and David G. Post, Law and Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1367 (1996).

4 See, *inter alia*, Tribunal de Grande Instance de Paris, 20.11.00., *LICRA et UEJF c. Yahoo! Inc. et Yahoo France*, ordonnance de référé du 20 Novembre 2000; High Court of Australia, 10.12.02, *Dow Jones & Co Inc. v Gutnick*, [2002] HCA 56. For more details on how and why courts have decided to exercise their jurisdictional powers over acts committed on the Internet, see Jack Goldsmith / Tim Wu, *Who Controls the Internet? : illusions of a borderless world*, 2006, Oxford University Press.

5 See for example Dan Jerker B. Svantesson, *Private International Law and the Internet*, 2nd ed., Kluwer Law International 2007.

- Business to consumer contracts (proposals 1, 3, 4).
- Personality torts (proposals 2, 3, 4).
- Intellectual property infringements (proposals 2, 3, 4).

Proposal 1: Internet-specific considerations should only apply if needed

- Issue at stake:
  - The fact that the Internet is relied upon as the basis for many contracts and torts should not, by itself, lead to the conclusion that all Internet-related litigation presents novel or challenging fact patterns. It is only in cases in which the distinguishing features of the Internet create uncertain results when deciding upon the jurisdiction of a court that the present principles should be reflected upon.
- Clarifications:
  - Appreciation of this proposal should be performed on a factual, case-by-case basis depending on the court seized and on the head used for determining its jurisdiction. Basically, it dictates that, when possible, Internet-specific considerations should be sidestepped.
- Examples
  - Company A, located in France, orders, against payment, some office supplies from the website of company B, located in Germany. If the supplies are deficient, the fact that the contract was concluded online does not affect in any way the fact that Company A may be able to sue Company B in Germany. Furthermore, the place of delivery of the goods – if not influenced by a clickwrap contract specifying otherwise – may be easily ascertained by its physical delivery in order to examine the jurisdiction of the courts located there.
  - Person A, located in Spain, orders, against payment, a game console through the website of company B, which is located in Austria. The fact that company B clearly does business with consumers located in Spain by performing delivery of goods there eliminates any hesitation one would have about the direction of its online activities.[6]
  - Newspaper A, which is available for purchase all across Europe and is also available through a website, publishes an indiscreet article about person B, an English national who resides there. Jurisdiction for a civil defamation suit in England and, for that matter, in other European countries would be legitimate regardless of the existence of the website because these locations are already the offline place of publication of the article.

Proposal 2: Rejection of jurisdiction based on website access

- Issue at stake:
  - In several leading cases regarding torts committed on the Internet, jurisdiction has been found appropriate over foreign websites due to the fact that they were made accessible to users located in the forum; the rationale being that any person who puts up a website on the Internet is aware of its global nature and should thus be ready to go to court wherever that site may be consulted.[7]

---

[6] This argument is in line with the standard of a commercial activity directed towards the domicile of the consumer, as stated in art. 17 (1) of the Brussels I Regulation (recast), for more on this, see Principle 4, below.

[7] *Dow Jones & Co Inc. v Gutnick* (note 4); Court of Appeal, Civil Division (England), 19.10.04, *Lewis & Ors v King*, [2004] EWCA Civ 1329; Cour de cassation, 1ère Chambre Civile (France), 09.12.03, *Sté Castellblanch c. Sté Champagne L. Roederer*, Arrêt num. 1637 FS-P+B. See also United States District Court, D. Connecticut, 17.04.96, *Inset Systems Inc. v. Instruction Set Inc*., 937 F.Supp 161.

- In the European Union, accessibility of a website is sufficient for triggering jurisdiction at the place of damages under article 7(2) of the Brussels I recast Regulation. The European Court of Justice has adopted this principle as regards to copyright and personality torts, in the *Pinckney*[8] and *eDate*[9] decisions respectively.
- This approach should be rejected. It ignores that many globally available websites, such as teen blogs, local and regional businesses and news sites, or personal websites do not seek global attention. It creates a risk of forum shopping and allows any court to enjoy universal jurisdiction over all websites which do not specifically make use of technological ways of filtering users.[10]
- In both *Pinckney*[11] and *eDate*[12], jurisdiction based on the accessibility of a website is limited to local damages only; according to the European Court of Justice, this curbs forum shopping because claimants should be naturally discouraged from engaging proceedings in jurisdiction where harm has been minimal and where they may consequently only recover paltry sums. However, practical evidence in the field of online defamation has shown that forum shoppers are not actually concerned with the quantum of damages as they rely on the mere threat of a lawsuit made abroad to pressure websites into settlement or into compliance.[13] Furthermore, the limitation fails to address the waste of judicial resources and the inefficiency that result from such a widely distributed jurisdictional head.
- Outside of EU community law, the accessibility standard has been mostly discredited and abandoned.[14]

- Examples:
  - Newspaper A, which is only circulated in the United States, yet is available through a website, publishes an indiscreet article about person B, a Greek national domiciled in that country. Person B seeks to sue Newspaper A in England, where he has no

---

8 European Court of Justice, Fourth Chamber, 03.10.13, *Peter Pinckney v KDG Mediatech AG*, case C-170/12.

9 European Court of Justice, Grand Chamber, 25.10.11, *eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited*, joined cases C-509/09 and C-161/10, European Court Reports 2011 I-10269.

10 For more details on these possibilities, see *Private International Law and the Internet* (note 5), at 320-352.

11 *Peter Pinckney v KDG Mediatech AG* (note 8), at 45. As for trademarks, see European Court of Justice, First Chamber, *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH*, Case C‑523/10.

12 *eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited* (note 9), at 43; this rule of distribution of damages is also applicable to physical publications, see European Court of Justice, 07.03.95, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA*., Case C-68/93, European Court Reports 1995 I-00415.

13 See for example Ministry of Justice (England), 23.03.10, Report of the Libel Working Group, 4-7 and spec. par. 10 ("Evidence from members of the Working Group indicated that a substantial reason for concern about libel tourism relates to threats of proceedings which in themselves may have a chilling effect on publication"). This impact assessment report on the practice of "libel tourism" eventually led to the abandonment of the accessibility approach in English law; see also the note just below.

14 *Inter alia*, see Cour d'Appel de Paris, 4ème Chambre A, 26.04.06, *SA Normalu c. SARL Acet*, num. 05/05038; Cour de Cassation, Chambre Commerciale (France), 09.03.10, *Delticom c. Pneus Online Suisse*, < http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2948> ; High Court of Justice, Chancery Division (England), 20.12.99, *1-800 FLOWERS Inc. v. Phonenames Ltd*., [2000] E.T.M.R. 369; High Court of Justice, Chancery Division (England), 25.07.00, *Euromarket Designs Incorporated v. Peters*, [2000] E.T.M.R. 1025; United States Court of Appeals, Fourth Circuit, 05.12.00, *Young v. New Haven Advocate*, 15 F.3d 256 (2002). See also article 9 of the English Defamation Act 2013, which was enacted in response to the problem of forum shopping in defamation suits: "A court does not have jurisdiction to hear and determine an action to which this section applies unless the court is satisfied that, of all the places in which the statement complained of has been published, England and Wales is clearly the most appropriate place in which to bring an action in respect of the statement".

permanent presence but has been known to the general public in the past; however, the website has only been consulted around 10 times by users there. The fact that it is accessible from England should not be deemed sufficient for the English Court to assume jurisdiction over a defamation claim.[15]

- Company A, a winery located in France, has commercialized a wine named C in France, where it has registered the trademark for that product. Company B, located in Spain, holds the trademark for an identically-named wine C in Spain. It operates a promotional website, which available globally but is entirely written in Spanish and refuses delivery to non-Spanish users. The fact that the website is accessible from France should not be deemed sufficient for the French court to assume jurisdiction over a trademark claim.[16]

Proposal 3: Rejection of automatic jurisdiction at the place of the claimant's domicile or habitual residence.

- Issue at stake:
  - In its 2011 *eDate* decision on online defamation, the European Court of Justice allowed for automatic jurisdiction of the courts situated at the place of the "centre of interests" of the victim, under the rationale that these are in the best position to take account of reputational harm done to a person.[17] Outside of this specific area of law, it could be argued that introducing a generalized "home country rule" would be a simple, efficient, and elegant way of resolving jurisdiction over torts committed over the Internet.
  - It is true that in most situations, jurisdiction of the courts of the domicile or habitual residence of a victim – places which will more often than coincide with *eDate*'s "centre of interests" standard – will be appropriate. However, it is difficult to go as far as to construe this preference as an *automatic* rule conferring jurisdiction to those courts regardless of whether any actual harm has occurred there.[18]
- Clarification
  - Instead of operating as an independent and automatic jurisdictional head, preference for a tort victim's home courts should be folded into the targeting test advanced in Proposal 4.
- Examples:
  - Website A, which is made available to users in the United States, and relies on technical means to block access to users in the European Union, publishes an indiscreet article about person B, a French national and resident having the centre of her interests there. French courts should not have jurisdiction over this case because no publication, and thus no harm, has occurred in France.
  - Website A, a personal website written in French, read by a French audience and owned by a French national with no real contact with the United States, publishes a user-made video which may possibly infringe the copyright held by company B, located in the

---

15 The facts of the example are inspired by High Court of Justice, Queen's Bench Division (England), 17.12.08, *Mardas v New York Times Co.,* [2008] EWHC 3135 (QB). In that case, use of the accessibility standard led the English court to consider that jurisdiction was appropriate.

16 The facts of the example are inspired by *Sté Castellblanch c. Sté Champagne L. Roederer* (note 7). Again, use of the accessibility standard led the French court to consider that jurisdiction was appropriate.

17 *eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited* (note 9), at 50. The court having jurisdiction at that place may adjudicate all of the worldwide damages.

18 Under the "place of harm" standard of art. 7(2) of the Brussels I Regulation (recast), direct harm is required in order to activate jurisdiction, see European Court of Justice, Sixth Chamber, 11.01.90, *Dumez France SA and Tracoba SARL v Hessische Landesbank and others*, Case C-220/88, European Court Reports 1990 I-00049; European Court of Justice, Fourth Chamber, 19.09.95, *Antonio Marinari v Lloyds Bank plc and Zubaidi Trading Company*, Case C-364/93, European Court Reports 1995 I-02719.

United States. Due to the lack of contacts between the website, its owner, its public and the United States, jurisdiction should not be deemed appropriate before the courts located at the place of the establishment of company B.

Proposal 4: Adoption of a targeting test

- Clarification
  - By "targeting test" it is meant an analysis of whether or not a website directs, or targets, its activity towards the forum.
  - Regarding contracts, the main use of targeting will arise when considering consumer contracts. In this context, the assessment of targeting is more precise, as it rests on whether the professional knowingly led its activity at the place of the consumer's domicile.[19]
  - When it comes to torts, the targeting test should play a role in determining jurisdiction at the place of damages. For personality torts, the test should be construed as striking a balance between the geography of the reputation of the victim and the foreseeable impact of the offending Internet content. Regarding intellectual property infringements, the targeting analysis should take into account the territorial nature of the intellectual property right in question in light of the remedy sought by the IP holder.[20]
  - One issue commonly associated with the targeting approach is its vagueness.[21] Indeed, in order for the test to provide certainty when it comes to determining whether or not a given forum is appropriate, it needs to be stated clearly and applied by courts in a cohesive manner.
  - In order to reach that goal, the following guidelines are submitted.[22]
    - The targeting test should be considered as assessing whether or not a website holds sufficient contacts with the forum. By contrast, its aim is not to determine which forum would be the most appropriate for a given dispute.
    - The requirement that a website should direct its activity towards the forum does not mean that its owner needs to have intentionally targeted the forum. To meet the standard, it will be sufficient to show that the website's structure and/or business model makes it objectively foreseeable that there would be a public in that place.[23]

---

19 In European law, a targeting test is used to determine whether the clients of an online trader located in a specific Member State have been targeted as consumers in that State, and thus whether they may make use of consumer status under the Brussels I Regulation (recast); see European Court of Justice, Grand Chamber, 07.12.10, *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller*, Joined cases C-585/08 and C-144/09, European Court Reports 2010 I-12527. At par. 50, the ECJ construes the targeting test as an analysis of whether "there [is] evidence demonstrating that the trader was envisaging doing business with consumers domiciled in other Member States [than the State of its establishment], including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with those consumers."

20 For examples of application of the targeting test to trademark disputes in particular, see *1-800 FLOWERS Inc. v. Phonenames Ltd*. and *Euromarket Designs Incorporated v. Peters* (note 14); see also WIPO, Joint Recommendation Concerning Provisions on the Protection of Marks, and Other Industrial Property Rights in Signs, on the Internet, 845(E) (2001); American Law Institute, Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes (2008), § 204.

21 Thomas Schultz, Carving up the Internet, Jurisdiction, Legal Orders and the Private/Public International Law Interface, European Journal of International Law, Volume 19 (2008), No. 4, 799, at 818-819.

22 For a detailed proposition of how an ideal targeting test could be structured, see Michel Reymond, Jurisdiction in Case of Personality Torts Commited over the Internet: A Proposal for a Targeting Test, Yearbook of International Private Law, Volume 14 (2012/2013) 205.

23 The proposed approach thus rejects the test used in United States Court of Appeals, Fourth Circuit, *Young v. New Haven Advocate*, 15 F.3d 256 (2002), requiring at 263 that an online newspaper "manifest an intent to target and focus on [the

- In order to give weight to this assessment, the following criteria may be used:
  - The language used by the website.
  - The website's access numbers by jurisdiction.
  - The website's search engine ranking and visibility when queried from the forum
  - The website's choice of top level domain
  - The website's topicality, when contrasted with the interests of the public of the forum.
  - The possibility for users located in the forum to use the website's services.
  - The website's use of technical means of filtering users by jurisdiction.
  - The website's use of targeted advertising.
- In line with the arguments brought forth in Proposal 3, the targeting test analysis should be contrasted against the forum's general relationship with the dispute. For example, in the case of online defamation, the court situated at the "centre of interests" of the victim should only reject jurisdiction if there is a showing that no direct harm took place there. By contrast, a court situated in a place where the victim has less presence should require a stronger degree of targeting.

o Examples
- Magazine A, which is circulated in the United States, but is also available globally through a website, publishes a defamatory article about person B, an Australian businessman domiciled in the State of Victoria.[24] Because Magazine A's website rests on a paid subscription model which has deliberately been made available to readers in Victoria, and furthermore because that place is the victim's centre of interests, the targeting element is fulfilled and jurisdiction of the local courts is appropriate.
- Website A is a music streaming platform based in the United States; it is available globally and in particular in Spain. Streaming is free, yet supported by unskippable audio advertisements. Artist B, based in Madrid, recognizes that one of her songs is present on the platform without authorization. Given the global ad-supported business model of Website A, artist B may file a copyright suit before the courts of Madrid, but also before any court in any jurisdiction in which the song has been made available.
- Restaurant A is located in France and operates a promotional website available globally, including in Germany. Restaurant B, operating under the same trademarked name which it has registered in its home country, wishes to sue Restaurant A for infringement. Depending on whether the website is available in German, owns a web address ending in .de and/or offers information and promotions targeted to a German audience, jurisdiction may be appropriate in Germany.

* * *

forum] readers" to be fulfilled; closer in nature to the proposed framework, see Opinion of Advocate General Cruz Villalòn, *eDate Advertising GmbH v X and Olivier Martinez and Robert Martinez v MGN Limited*, Joined Cases C‑509/09 and C‑161/10, at 59-65 and spec. 62. For more on these two strands of targeting, see also Valérie Pironon, Dits et non-dits sur la méthode de la focalisation dans le contentieux – contractuel et délictuel – du commerce électronique, Clunet 2011/4, 915, at 920-923.

[24] The facts of the example are inspired by *Dow Jones & Co Inc. v Gutnick* (note 4). The High Court of Australia in that case concluded that jurisdiction was appropriate based on the sole availability of the website in Victoria.

Topic 2

How to structure an alternative dispute resolution system for Internet-related disputes?

Introduction and presentation of the procedural framework proposal

- The rise of social networking platforms and the continued importance of search engines give rise to a high number of potential infringement cases[25] which would involve parties from various jurisdictions around the world.

- In addition to issues pertaining to territoriality (see Session 1), traditional dispute resolution mechanisms are unfit to deal with the large number of potential infringements on the Internet (whether related to IP, privacy, personality, or other rights) and may not be easily accessible to the general public.

- Alternative dispute resolution mechanisms exist for specific Internet-related disputes, e.g. the UDRP (for domain name disputes), the DMCA's notice and takedown system (for copyright infringement in the USA), and the EU Online Dispute Resolution for consumers and traders related to goods or services purchased online.

- Some operators of the Internet have adopted dispute resolution mechanisms on their own initiative (e.g. Facebook and Twitter for trademark related disputes) or based on legal or judiciary requirements (e.g. Google as regards its "European privacy requests for search removals"). However, these dispute resolution mechanisms remain unclear/opaque – as regards the rules they are based on and the way they are examined by the operators – and may not best serve all the interests at stake.

- This proposal for an alternative dispute resolution system for Internet related disputes (**"pADR"**) aims at remedying the aforementioned shortcomings by providing a procedural framework and principles, which would be applicable to any kind of Internet related dispute.

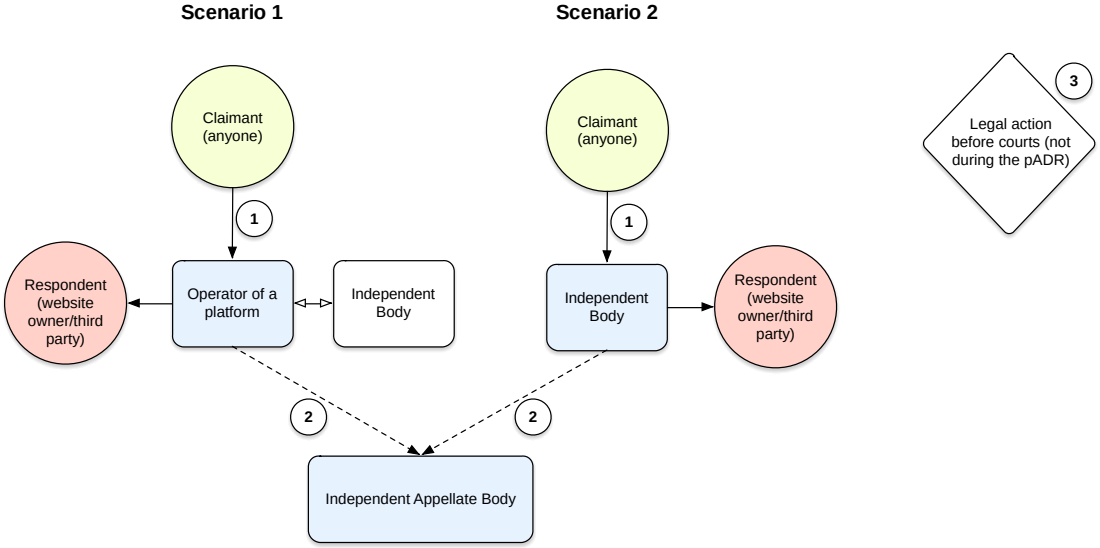
- This procedural framework takes into account the two following scenarios:

    - Scenario 1: the potential infringement is the result of material that was published by a third party on an Internet platform/website that it does not operate (e.g. a content posted by a Facebook user on her Facebook page) or third party material that is directly or indirectly referenced on an Internet platform/website (e.g. the link to a third party website which is referred to on a Google search result page).

[25] By way of example, Google's Transparency Report states that Google has examined (i) 480,569 requests for removal of links based on the "right to be forgotten" since May 29, 2014 (https://www.google.com/transparencyreport/removals/europeprivacy/; last updated on July 25, 2016) and (ii) 84,214,923 URLs requested to be removed from its search engine based on copyright infringement since 2011 (https://www.google.com/transparencyreport/removals/copyright/?hl=en; last updated on July 25, 2016).

- Scenario 2: the potential infringement is the result of material that was published on a website by the operator of such website or by any person under such operator's responsibility (e.g. an article authored by an employee of a journal which is published on the journal's website).

- An overview of the proposed procedural framework is reproduced below.



- Comments on the procedural framework proposal:

(1) In case of infringement, a claimant may file a request to the operator of a platform (in scenario 1) or to the Independent Body (in scenario 2), which will be the first entity to decide on an infringement case.

In scenario 1, as the operators (i) are responsible for setting up a platform where infringements by third parties may take place and (ii) have the technical know-how to deal with a high number of cases (by automating parts of the processing of requests), it is justified that they should bear the responsibility of being the first entity to decide on an infringement case. In addition, the operators would be incentivized to implement the pADR, as they would benefit from a safe harbor (see below). Upon request of the operator, the Independent Body may provide guidance to such operator on a case by case basis.

In scenario 2, the Independent Body shall decide on infringements cases, as there are no platforms involved.

For the avoidance of doubt, the Independent Body laid out in scenarios 1 and 2 shall be the same entity (with different roles depending on the scenario), which shall be created for the purpose of this pADR.

(2) In scenario 1, the claimant, the respondent and, in case of public interest, the Independent Body shall have the right to appeal the decision of the operator of the platform to the Independent Appellate Body.

In scenario 2, the claimant and the respondent shall have the right to appeal to the Independent Appellate Body.

The Independent Appellate Body could be an entity already existing (e.g. the WIPO Mediation & Arbitration Center) or a new entity to be set-up for the purpose of the pADR.

(3) The pADR shall be exclusive of other dispute resolution mechanisms. This means that at the moment when a claimant files a request under the pADR and until the process under the pADR is concluded, such claimant opts in to such exclusive alternative dispute resolution and is thus prevented from bringing the same case before national or regional courts until the pADR procedure is over[26].

- The pADR shall not be mandatory, but rather be an alternative option – for the claimant as well as the respondent and the involved operator, if any – that would be incentivized by the following:
    - The principles of the pADR, in particular the accessibility (see proposal 1.1 below) would benefit both the claimants and the respondents;
    - the operators shall benefit from a safe harbor if they participate in and implement the pADR in accordance with all its principles and rules.

Principles

1. Proposals of procedural principles for the pADR

1.1 The pADR shall be accessible financially and procedurally (***Accessibility***).

- The costs of submitting a request using the pADR shall be low (e.g. USD 5) in order for anyone in the general public to be able to use it.
- The pADR shall not be unnecessarily burdensome procedurally to remain accessible to anyone without the help of a legal counsel. In order to simplify the submitting of a request, a model complaint for each kind of claims shall be made available for use by potential claimants[27].

1.2 In principle, each party related to a specific case shall have the right to be heard (***Right to be heard***).

- The parties related to a specific case are (i) the claimant and (ii) the respondent.
- As a matter of efficiency, a relatively short deadline shall be set for the respondent to submit a response (e.g. 5 business days).
- No further submission exchange shall be possible at the first stage (before the operator of a platform or the Independent Body). At the appeal stage, a second round of submissions shall

[26] Similarly to what Paragraph 4 (k) of the UDRP provides ("*[t]he mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from* ***submitting the dispute to a court*** *of competent jurisdiction for independent resolution* ***before*** *such mandatory administrative proceeding is commenced* ***or after*** *such proceeding is concluded*"; emphasis added).

[27] By way of example, the WIPO Arbitration and Mediation Center has prepared a model complaint for the UDRP (http://www.wipo.int/amc/en/domains/complainant/).

be requested by the appellant. A relatively short deadline shall be set to both parties in such case (e.g. 5 business days).

- In case of failure to meet a submission deadline, the decision-making entity shall be allowed to decide without hearing the respondent or the claimant (in case of further submissions).

- During the first stage of the pADR (i.e. until a decision granting the request of the claimant is taken by the operator or the Independent Body), the disputed material or content shall remain available online. During the appeal stage of the pADR, the content shall remain online if the request has been denied or shall remain offline if the request has been granted.

1.3 Each decision-making entity shall decide impartially on the basis of the facts and in accordance with the substantive principles without any restrictions, improper influences, inducements, pressures, threats, or interferences (***Independence***).

- The operators shall appoint specific personnel for such task which shall be relatively independent (similar to the role and status of a data protection officer as provided under EU law[28]).

- The independent body and independent appellate body shall be independent from the operators. However, their funding may partially be based upon contributions by the operators.

1.4 Both the procedural principles and the substantive principles shall be published and made available to the public; in addition, the Independent Body shall have access to all cases' data and shall regularly and publicly report on such cases (***Transparency***).

- The decisions would not all be published. At the first level, the decisions of the operators would be published only upon decision of the independent body. The decisions of the independent appellate body would all be published. This distinction allows filtering the decisions not to flood the public with too much information (which would hinder the clarity and transparency of the process).

- The Independent Body shall regularly publish a "transparency report" containing statistical/anonym information related to cases decided under the pADR.

- Notwithstanding the preceding: (i) decisions pertaining to the "right to be forgotten" or other privacy matters shall in principle be redacted to the extent required to anonymize the claimant before they are made public and (ii) other decisions shall be redacted upon request of the concerned party in order to accommodate its rights/interests.

[28] See inter alia Article 24.7 of Regulation 45/2001 which states: "*[w]ith respect to the performance of his or her duties, the Data Protection Officer may not receive any instructions*".

2. Proposals regarding substantive rules applicable in the context of the pADR

2.1 A set of substantive rules shall be drafted by "dumbing down" internationally recognized principles (i.e. finding the common denominator).

2.2 The substantive rules shall be different and adapted to each subject matter (e.g. copyright, trademark, personality rights, "right to be forgotten").

2.3 The same substantive rules shall be applied by all decision-making entities.

* * *

Topic 3

How shall disputes about the licensing of Standard Essential Patents (SEP) under Fair, Reasonable and Non-Discriminatory (FRAND) terms be solved?

Introduction

- Standards and standard setting organizations ("**SSO**") have always played a key role in the ICT sector. Quite obviously, the selection of a technology as part of a standard generally provides a competitive advantage to its owner, as the technology becomes technically essential in order to implement the standard. In case there is no true alternative standard available on the market, the incorporated technology is not only technically but also commercially essential, providing in substance a dominant position to its owner.

- Over the last decade, disputes in the ICT industries have increasingly been centered around requests made by IPR owners whose technology has been incorporated in a standard preventing the use of their rights by third party users (so-called implementers) or claiming allegedly excessive compensation for the use of this technology. Even if such disputes are of civil nature in the first place, competition authorities have increasingly jumped in (often upon request of potential licensees) on the ground that IPR owners are trying to corner the market or getting overly high return in consideration for the use of the technology and, as a consequence, that said IP owners are slowing down the diffusion of technology and preventing effective competition from taking place. Hence, both private and public interests are at stake in modern disputes in the ICT industries. [1]

- In order to address these concerns, SSOs have typically adopted IPR policies whose main purpose is to request from IPR owners that they commit *ex ante* to license their technologies on fair, reasonable and non-discriminatory terms (usually referred to as FRAND or RAND terms in practice) in the event these technologies are incorporated in a standard. From a theoretical perspective, the concept of FRAND terms is relatively easy to grasp. By contrast, the practical determination of what would constitute, for instance, a fair or reasonable royalty for the use of the technology incorporated in a standard is a much more delicate issue.

- We believe that disputes in the ICT industries relating to FRAND terms would be more efficiently solved with the ADR mechanism proposed below. [2] This mechanism should not be

---

[1] In the EU, see for instance EU Commission, *Samsung - Enforcement of UMTS standard essential patents* (Case COMP/39.939), and, more importantly, ECJ, *Huawei v. ZTE* (Case C-170/13). For a critical review of this latter case, see notably RATO M./ENGLISH M., *An Assessment of Injunctions, Patents, and Standards Following the Court of Justice's Huawei/ZTE Ruling*, in: Journal of European Competition Law & Practice, 2016/2, p. 103 et seq. In the US, see recently United States Court of Appeals for the Ninth Circuit, *Microsoft Corp. v. Motorola, Inc.*, Case No. 14-35393. For a review of this case, see for instance PAUL J./KACEDON D. B., *Recent U.S. Court Decisions and Developments Affecting Licensing*, in: Les Nouvelles, 2015/4, p. 237 et seq. (in particular p. 240). With respect to China, see ZHOU Z., *New Chinese Rules on Abusing IPRs: What Does It Mean for the Exercise of IPRs after the Qualcomm Case*, in: World Competition 2015, p. 597 et seq. (in particular p. 601 et seq. on the *Qualcomm* case). See also, OECD, *Intellectual Property and Standard Setting – Note by the United States*, DAF/COMP/WD(2014)116.

[2] For the paper that may be considered as seminal in this respect, see LEMLEY M. A./SHAPIRO C., *A Simple Approach to Setting Reasonable Royalties for Standard-Essential Patents*, in: Berkeley Technology Law Journal, 2013, Vol. 28,

made mandatory. We rather aim at creating incentives within the mechanism to increase chances of players in the industry adopting it. In addition, the ADR mechanism proposed below aims at taking properly into account competition law issues and, thus, at being approved by competition authorities. As a result, such authorities should have no ground to intervene in disputes relating to FRAND terms. These incentives would be as follows:

  - For IPR owners, the main incentive for accepting the ADR mechanism proposed below would be the non-intervention of competition authorities (provided that certain conditions are met). Also, IPR owners would expect their rights to be fairly valued in the context of the proposed ADR mechanism.
  - For potential licensees, the main incentive would be the low cost/ease of use of the procedure. Also, potential licensees would have an interest in the fact that they would be protected against injunctions from civil courts preventing them from using the technology incorporating the standard. Potential licensees would expect a fair value to be attributed to their use of the technology.
  - For the SSOs, the incentive would stem from the fact that FRAND disputes would be more efficiently solved and this would accelerate the diffusion of the standard in the market. In addition, under the proposed mechanism, SSOs would not need to be involved in determining what constitute FRAND terms. Last, SSOs would be immune from competition law liability, which may otherwise be engaged in the event SSOs fail to set up a mechanism for solving disputes (absent such system, SSOs may be considered as assisting powerful undertakings in holding up the standard).
  - For competition authorities, the incentive would reside in the fact that they would not have to deal with complex investigations with uncertain outcome, while at the same time the system would ensure that efficient competition is not impeded.

- For the avoidance of doubt, the purpose of the system would be the efficient resolution of cases and not necessarily the harmonization of laws at a global level.

- Links with other sessions:
  - Since Sessions 2 and 3 both contemplate ADR mechanisms, they share a number of common features. That said, the ADR mechanism proposed below relies, unlike Session 2 which may technically rather qualify as mediation, on arbitration *stricto sensu*.

1/ Proposals for an ADR mechanism for solving disputes relating to FRAND terms

- **Proposal 1.1: Participation by companies in the standardization process should be conditional upon accepting an ADR procedure in case of future disputes relating to FRAND terms.**
  - Comments:
    - The submission of future disputes relating to FRAND terms to an ADR procedure should be set out in the IPR policies of SSOs and companies willing

p. 1135 et seq. See also the section dedicated to FRAND disputes in DE WERRA J., *Patents and trade secrets in the internet age*, in: Revue de droit suisse 2015, p. 123 et seq. For examples of ADR procedures applicable to FRAND terms disputes, see WIPO Arbitration for FRAND Disputes (http://www.wipo.int/amc/en/center/specific-sectors/ict/frand/annex1/) and WIPO Expedited Arbitration for FRAND Disputes (http://www.wipo.int/amc/en/center/specific-sectors/ict/frand/annex2/).

to participate in the standardization process should accept to comply with these IPR policies.
        - The ADR procedure should be an arbitration procedure *stricto sensu* ending with a binding arbitration award. Should a mediation process be proposed, it should be subject to a strict time limit and end up by a binding and immediately fully enforceable agreement.
        - The procedure could be managed either within the SSO or outside the SSO (in this case, the IPR policies should specifically refer to one or several selected management organisms such as the WIPO Arbitration Center).

- **Proposal 1.2: The ADR procedure in case of future disputes relating to FRAND terms should be a fast track ADR procedure.**
    - Comments:
        - The fast track ADR procedure should be based in particular on the following principles:
            - The briefs filed by the parties should not exceed a defined number of pages.
            - The parties should be limited in terms of expert reports they could file in support of their briefs.
            - Strict time limits should govern the ADR procedure.
            - The arbitration tribunal should not be entitled to request its own additional expert reports.
            - The arbitration tribunal could set FRAND terms different from those submitted by the parties.
            - The procedure should set forth an appeal:
                - The appeal procedure should be similar to the procedure governing the first instance.
                - The appeal should be limited to legal errors and procedural deficiencies.

- **Proposal 1.3: Decisions issued at the end of the ADR procedure should be partially published.**
    - Comments
        - Issues at stake:
            - Full publicity of decisions could be problematic, especially from the patent owners' perspective, who would rather keep both the ADR procedure and the content of the decision secret.
            - Non-publicity could be an issue for the public and competition authorities (as they would not be in a position to ensure that FRAND terms have been ordered).
        - Partial publicity means that decisions should disclose the names of the parties and the methodology relied upon by the arbitration tribunal to arrive at specific FRAND terms, but shall in no event disclose specific terms.
        - Partial publicity also means that the non-confidential version of the decision should disclose the fact, if it occurs, that the IPR owner has infringed competition law (see Section 2.2 below which clarifies the conditions under which the IPR owner can be shielded from competition law liability).

- The non-confidential version of the decision should be published within a reasonable timeframe (e.g. 90 days following the issuance of the decision).

- **Proposal 1.4: The ADR procedure should be the unique way to solve the legal issues pertaining to these rights and the parties should not be allowed to interfere with this procedure in any manner. In particular, owners of technically essential IPR should not be allowed to seek an injunction from an ordinary court aiming at blocking the use of the technology while the ADR procedure is pending (including in case of an appeal). In addition, the ADR procedure should not offer owners of technically essential IPR the opportunity to seek an injunction aiming at blocking the use of the technology.**
  - Comments:
    - Rationale: given that the adoption of a technology in a standard is in principle subject to the obligation to license the technology under FRAND terms, seeking an injunction aiming at blocking the use of said technology seems hardly justifiable. Seeking an injunction in such setting seems inconsistent with the commitment to license the technology. Therefore, the remaining issue should only be the determination of the FRAND terms.
    - If an injunction is sought from an ordinary court while the ADR procedure is pending, the ordinary court would have to grant a stay since the parties agreed to the ADR procedure before starting litigation or arbitration.

2/ Proposals regarding substantive rules applicable in the context of ADR procedures within the meaning of Section 1 above

- **Proposal 2.1: Infringement as well as validity and enforceability of IPRs should be assessed based on the choice of law made by the parties and, absent such choice, on the law with which the case has the strongest connection.**

- **Proposal 2.2: Owners of IPR should be shielded from competition law liability when seeking compensation for the use of their technology, provided however:**
  - **Alternative 1: Owners of IPR have served a prior notice detailing the alleged infringement and proposing fair terms for a license (in particular the royalty and the factors underlying its calculation, including supporting documentation).**
    - Comments:
      - Rationale: the exemption from competition law liability would increase the incentive of IPR owners to join SSOs requesting the participation in fast track ADR mechanism in case of disputes relating to FRAND terms.
      - The question whether fair terms have been proposed in the prior notice should not be assessed too restrictively. Otherwise, the incentive provided to the IPR owner would be inefficient. For the sake of clarity, the terms proposed may differ from the terms that would be determined by the arbitration tribunal (or the appellate court) at the end of the procedure, but only to a reasonable extent. In the event the terms proposed appear to be significantly higher than the terms established in the decision, the competition law liability of the IPR owner would be triggered (that said, the arbitration tribunal or the appellate court would obviously not have the power to issue fines).

- **Alternative 2: Owners of IPR demonstrate that they do not hold a dominant position (i.e. their technology is technically but not economically essential).**
  - Comment:
    - This alternative aims at taking into account economic as well as competition law considerations. If the right holder can demonstrate that it does not hold a dominant position because sufficient alternative technologies are available on the market (i.e. the patent is essential from a technical but not a commercial perspective), it is not justified to consider that the right holder has breached competition law.

3/ Proposals for coordination with competition authorities

- **Proposal 3.1: The fast track ADR procedure described under Sections 1 and 2 above should be considered as compliant with legitimate requirements of competition law and, therefore, competition authorities should not intervene unless the IPR owner has not complied with one of the alternatives set out in Proposal 2.2.**
  - Comment:
    - The ADR procedure described in Sections 1 and 2 aims at reaching a right balance between various interests, including the protection of efficient competition. Should such ADR procedure be set up and should the IPR owner comply with its requirements, competition authorities should be unwilling to take cases (principle of opportunity).

- **Proposal 3.2: In the course of the ADR procedure, the arbitration tribunal/the appellate court could seek an opinion – on a no-name basis – from one or several major competition authorities if a question of principle arises.**

* * *

Topic 4

—

How shall immunities apply on the Internet?

Introduction: The continuing applicability of the international law and domestic law framework governing immunities and of properties (state and international organizations)

- The emergence of new social facts does not as such render obsolete the existing applicable rules of international law. However, new social facts may give rise to new practices, which becomes rules of international law either through implicit or express consent. For instance, the creation of nuclear weapons after the Geneva Conventions and customary international law did not render obsolete the rules of international humanitarian law.[1] The same goes with the Internet. Neither the development of the Internet nor its increasing pervasiveness in contemporary daily life changes the general regime of international law, including the rules governing the immunities applicable to states and international organizations. As a practical consequence, existing rules of international law, both customary and conventional, applicable to state immunities continue to govern legal relations falling within their scope of application.

- A state can therefore invoke its sovereign immunity as a bar to legal proceedings for activities it conducts in it acts in its sovereign capacity. *Par in parem non habet imperium*. However, when a state acts in its private capacity, engaging in *acta iure gestionis*, that is to say as a private person, it cannot avail itself of immunities.[2]

- State immunity also protects high-ranking state officials under customary international law for their time in office.
    - Incumbent state presidents, prime ministers, and ministers of foreign affairs can also invoke their state's immunities for acts committed, even when such acts were not attached to their functions.[3]
    - An emerging trend of case law considers that incumbent high-ranking state officials' immunities do not apply before international tribunals and courts, such as the International Criminal Court.[4]
    - It is however difficult in practice to determine how high-ranking state officials may be involved in Internet-related violations of international law.
- Other state officials may enjoy immunities when in mission in foreign states.[5]
- Other state agents may enjoy *ratione materiae* state immunities for acts that they perform in their official capacity.

---

1 See on this issue, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, paras. 86-87.

2 Article 10 of the United Nations Convention on Jurisdictional Immunities of States and Their Property, New York, Dec. 2, 2004, UN Doc. A./RES./59/38. (The Convention is not yet in force. However, the provisions we rely upon are of a customary international law nature)-

3 *The Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*, Judgment, I.C.J. Reports 2002, para. 51.

4 See for instance, International Criminal Court, Pretrial I Chamber, *The Prosecutor v. Al. Bashir (Decision Pursuant to Article 87(7) of the Rome Statute on the Failure by the Republic of Malawi to Comply with the Cooperation Requests Issued by the Court with Respect to the Arrest and Surrender of Omar Hassan Ahmad Al Bashir)*, Dec. 12, 2011, para. 43.

5 See the United Nations Conventions on Special Missions, New York, Dec. 8, 1969, 1400 U.N.T.S. 231.

- State immunities also cover state property 'affected to a non-commercial purposes', including their Internet-related components.[6] As such, state properties not affected 'affected to a non-commercial purposes', included their Internet-related components, are immune of measures of constraints, such as attachment.[7]
    - Warships,[8] assets serving diplomatic[9]and consular purposes[10], and the assets of central banks[11] have traditionally been considered as state properties affected 'affected to a non-commercial purposes', and – enjoying therefore immunities from measures of constraints under international law.
    - Other assets may be covered by state immunity according to their destination.

- Although new social facts, such as the Internet, do not as such affect the existence of pre-existing normative regimes. However, they engender new issues, especially as to the applicability and the application to them of pre-existing normative regimes, calling therefore for clarifications.

1./ Fostering the respect of foundational principles of international law

Proposal 1.1: State agents do not enjoy immunity for Internet-related crimes committed on third states' territory, except acts committed by military forces in period of armed conflict.

- State agents enjoy *ratione materiae* immunity for state acts, that is to say, acts they perform in their official capacity. As *ratione materiae* immunity relates to the state act itself, and not to the state agent, a state official can avail himself of such immunity even after their time in office. Exceptionally, however, a state agent may not enjoy immunity for acts committed in her official capacity when such acts are committed in foreign territory. Article 12 of the *United Nations Convention on Jurisdictional Immunities of States and their Property*, codifying in some respect, what is known as the 'territorial tort exception', stipulates:

    > 'a State cannot invoke immunity from jurisdiction before a court of another State which is otherwise competent in a proceeding which relates to pecuniary compensation for death or injury to the person, or damage to or loss of tangible property, caused by an act or omission which is alleged to be attributable to the State, *if the act or omission occurred in whole or in part in the territory of that other State and if the author of the act or omission was present in that territory at the time of the act or omission*.' (Emphasis added)

- State practice does not unanimously recognize the territorial tort exception.
    - On the one hand, some domestic jurisdictions have opined that state agents do not enjoy immunities for breach of international and domestic law committed outside their territory. Thus, France intelligence agents that sank Green Peace's vessel, the *Rainbow*

---

6 Articles 18 and 19, United Nations Convention on Jurisdictional Immunities of States and Their Property.

7 *Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening)*, Judgment, I.C.J. Reports 2012, para. 118.

8 Article 32 of the 1982 United Nations Convention on the Law of the Sea; *ARA Libertad (Argentine Republic v. Ghana)*, Provisional measures decision, Dec. 15, 2012, para. 95.

9 Article 22 Vienna Convention on Diplomatic Relations, April 18, 1961, 500 U.N.T.S 95.

10 Various articles, including Article 59, United Nations Convention on Jurisdictional Immunities of States and Their Property.

11 Article 21, *ibid*.

Warrior, in the territorial waters of New Zealand, did not enjoy immunity before New Zealand's domestic courts.[12]

- On the other hand, the European Court of Human Rights questioned the 'universality' of the territorial tort exception.[13] In addition, on the basis of a review of state practice, the International Court of Justice pointed out that under customary international law, state armed forces enjoy immunities for torts committed outside their national territory in the context of an armed conflict.[14]

- The difficulties surrounding the 'territorial tort exception' to state *rationae materiae* immunity increase with respect to the Internet for at least one main reason. As much as the Internet reduces time and space, in some cases, it disconnects the place of an action from that of its effects. Concretely, Internet allows infringing another state's territorial sovereignty and rights without the actor being physically on its territory. Spying, cyber-attacks, and other Internet-related offences do not require a physical presence on a foreign state territory. The separation between the place of an action and the place of its effects raises question on the applicability of the territorial tort exceptions in such circumstances.

- We propose that 'State agents do not enjoy state immunity for Internet-related crimes committed on third states' territory, except acts committed by military forces in period of armed conflict'.

- Three main reasons justify this policy proposal.
  - First, the policy proposal is consistent with international law. Using the Internet as a means to infringing other states' rights from abroad violates fundamental principles of international law, such as territorial sovereignty and non-intervention in other states' domestic affairs.[15] As a consequence, foreign interference in a territory under state sovereignty, including through enforcement actions, without its consent is a violation of international law.[16] Thus, the proposal promotes the maintenance of international peace and security by discouraging the violation of third parties' rights from abroad.
  - Second, depriving state agents of immunities for state acts which infringe third states' rights abroad does not create new legal obligations upon them and raises no concern regarding the principle of legality, a fundamental principle under (international) criminal law.
  - Third, the proposal does not run counter to usual definitions of the *locus delicti*. In general, domestic laws define the *locus delicti commissi* using both the place of commission of the act and that of its effect. Actually, the proposal simply removes the possibility that immunity may be conducive to impunity in this case.

- The controversies surrounding the application of the territorial tort exception to the acts of armed forces abroad in period of armed conflicts justifies the caveat in the proposal in this respect. As mentioned above, the International Court of Justice's review of state practice

---

12 *R. v. Mafart and Prieur* (1986) 74 International Law Reports 241; *R. Lambeth Justices, ex parte Yusufu*, [1985] Crim. L. R. 510.

13 *McElhinney c. Ireland* (2001) 123 ILR 73 at 85, para 38.

14 *Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening)*, Judgment, I.C.J. Reports 2012, para. 78.

15 GA/RES/25, Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.

16 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment. I.C.J. Reports 1986, para. 202.

considers that, under customary international law, armed forces enjoy immunities in these circumstances.[17]

1.2. Protecting the properties of states through immunities under international law

- The property under review at this stage is of two types:
    - First, it includes property, which undoubtedly qualifies, as state property themselves, such as embassies, central-banks funds, warships, and which enjoy immunities on their own stand, including their Internet related components.
        - This type of property and their Internet-related property do not raise particular problems-
    - Second, it includes internet-related objects which have a direct relation to an international organization or a state:
        - This is the case of country top level domain names (ccTLDs), which allow a website's web address, or 'URL' to be associated with a country specific alphanumeric string such as '.ch' for Switzerland, '.fr' for France or '.co.uk' for the United Kingdom.
        - This is the case also states and international organizations' second level domain names, when they are composed of their identifiers, such as names, symbols, or acronyms.
    - We are therefore not concerned with top level and second level domain names, which are not specific enough to refer to an identified state or international organization.
        - This section does not therefore deal with generic domain names, such as (.gov), (.edu), (.org) etc, which do not refer to a specific, identified, or determinable state or international organization.

Proposal 1.2.1: States domain names are per nature properties used for non-commercial purposes, and as such should enjoy immunities under international law

- Under international law, states enjoy immunity for their property used for a 'non-commercial purposes'. Thus, article 10 of the *United Nations Convention on Jurisdictional Immunities of States and Their Property* stipulates that:

> 'No post-judgment measures of constraint, such as attachment, arrest or execution, against property of a State may be taken in connection with a proceeding before a court of another State unless and except to the extent that: […]
>
> c) it has been established that the property is specifically in use or intended for use by the State for other than government non-commercial purposes and is in the territory of the State of the forum, provided that post-judgment measures of constraint may only be taken against property that has a connection with the entity against which the proceeding was directed.'

- International instruments do not as such define what a 'property' is for the purposes of state immunities. As a plea of state immunity has to be made before domestic courts and tribunals,

[17] See also, Article 31 of the European Convention on State Immunity, May 16, 1972, 1495 UNTS 182.

any definition of what constitutes a 'property' for the purposes of state immunity is to be found in the relevant domestic law on state immunity.

- In the *Ben Haim and al. v. Islamic Republic of Iran and al.*, the claimant requested ICANN to make available for attachment the domain names of Iran, Syria and North Korea's– '.ir', '.kp', '.sy', to satisfy judgments against these countries.
  - Appearing before the Court as non-party to the case, ICANN raised five objections to the request. The first objection maintains that country code top level domain names are not 'property' and could not, therefore, be subject to measures of constraint.
  - As a subsidiary argument, ICANN maintained that ccTLDs were not properties belonging to states, and that at any rate, if they were such a property, they would be protected by state immunities under the FSIA.
  - The US Supreme Court of the District of Columbia, on the basis of the applicable local law, upheld the first argument, without entering into the subsidiary argument of whether country code top level domain names are protected by state immunities:

    '*The ccTLDs exist only as they are made operational by the ccTLD managers that administer the registries of second level domain names within them and by the parties that cause the ccTLDs to be listed on the root zone file. A ccTLD, like a domain name, cannot be conceptualized apart from the services provided by these parties. The Court cannot order the plaintiffs' insertion into his arrangement*.'[18]
- For the DC Supreme Court, country code top level domain names possess as such no monetary value prior to their enlistment on the root zone file.
  - Attaching country code top level domain names could therefore not serve any purpose to the claimant, although such an action would disturb the normal functioning of Internet, and causing a great prejudice to private persons.
  - The position of the D. C. Supreme Court is consistent with various statements from stakeholders in the Internet community, which have held that domain names are no properties.[19]
  - Although the decision of the Supreme Court of the District of Columbia was limited to country code top level domain names, it could be extended by analogy to state second level domain names too.

- A better view on this issue would consider that state domain names are 'properties' available for attachment under the international law of state immunity, and therefore to be immune of any measure of constraints.
  - The reasoning should not be limited to the technical operation of listing a ccTLD on the rootfile, which requires the intervention of a registrar for the creation and exercise of rights relative to domain names.
    - Of more relevance is the apprehension of domain names by economic actors who ascribe to it an economic value, capable of ownership and of disposition, as much as any real property.[20]

---

[18] United States District Court of Columbia, *Ben Haim and al. v. Islamic Republic of Iran and al*., Nov. 10, 2014, 7.

[19] See, *Ben Haim and al. v. Islamic Republic of Iran and al. case*, ICANN's Memorandum to quash writ of attachment, 13

[20] On this argument, see Moe Alramahi, *The Legal Nature of Domain Names Rights*, 2009 (8) Journal of International

- In *Kremen v. Kohen*, the Ninth Circuit of the United States Court of Appeals emphasized that the notion of 'property' was a 'broad' one. Applying a three-part test to hold that domain names were 'property', the Court decided that:

  'Like a share of corporate stock or a plot of land, a domain name is a well-defined interest. Someone who registers a domain name decides where on the Internet those who invoke that particular name – whether by typing it into their web browsers, by following a hyperlink, or by other means – are sent. Ownership is exclusive in that the registrant alone makes that decision. Moreover, like other forms of property, domain names are valued, bought and sold, often for millions of dollars.'[21]

- Similarly to the Ninth Circuit of the United States Court of Appeals, the European Court of Human Rights was equally impressed by the 'economic value' arising from transactions regarding domain names.
  - In *Paeffgen v. Germany*, the Court was of the view that domain names constituted properties under Protocol I of the European Convention of Human Rights. For the Court:

  The contracts with the registration authority gave the applicant company, in exchange for paying the domain fees, an open-ended right to use or transfer the domains registered in its name. As a consequence, the applicant could offer to all Internet users entering the domain name in question, for example, advertisements, information or services, possibly in exchange for money, or could sell the right to use the domain to a third party. The exclusive right to use the domains in question thus had an economic value. Having regard to the above criteria, this right therefore constituted a 'possession', which the court decisions prohibiting the use of the domains interfered with.[22]

- Second, states seem to view their TLDs as property to be protected against private acquisition, and possessing economic values.
  - First, Article 6 *ter* of the Convention prohibits members of the Union from recognizing such emblems as trademarks or elements of trademarks. The provision suggests that state parties to the 1881 Paris Convention for the Protection of Industrial Property claim at least an entitlement to their identifiers.
  - Second, some states, such as Tuvalu have found their domain names economically profitable, licensing their use by private actors, against compensation.[23]

Trade and Policy 84, 88. See also, Yee K, *location.location.location: a Snapshot of Internet Addresses as Evolving Property*', 1997 (1) The Journal of Information, Law and Technology http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/yee.

[21] Kremen v. Cohen, 337 F. 3d 1024 - Court of Appeals, 9th Circuit 2003.

[22] European Court of European Rights, Fifth Section, *Paeffgen v. Germany,* Decision as to the Admissibility of Application nos. 25379/04, 21688/05, 21722/05 and 21770/05.

[23] *See* Jane Black, *Tiny Tuvalu Profits From Web Name*, (http://www.nytimes.com/2000/09/04/business/tiny-tuvalu-profits-from-web-name.html, visited on November 9, 2016).

        - Third, a few countries have begun archiving the Internet for use in their public libraries. Interestingly enough, in this context, state have decided that for the purpose of constituting a national archive of the Internet, a TLD based system is used. In the UK, the "uk web" will thus be any website using the .co.uk ccTLD.[24] This is an additional proof that States consider their own ccTLDs as closely linked to national identity and iconography.

    - Third, policy considerations justifies considering state domain names as properties for the purposes of state immunity.
        - In the absence of any restrictive definition of a property exists under international law, this approach has the advantage of uniformity and not to be dependent on the definition of a 'property' under different domestic laws.
        - Qualifying state names, symbols or acronyms as state property allow protecting of the TLD as such, independently of any use for IANA purposes.

- As state 'property' under the law of state immunities, domain names are immune against measures of constraints.
    - Only a waiver would authorize measures of constraints against its TLD.
    - Because of their critical importance to the maintenance of orderly international communications, similarly in this respect to diplomatic and consular assets which have been considered as requiring a specific waiver,[25] a waiver of immunity regarding TLDs should be specific, and not general. This would avoid a waiver to be inferred from poorly drafted clauses, and authorize judicial actions that would disturb the proper functioning of the Internet for a state and its population.
    - Domain names using state names, symbols or acronyms, are somewhat similar to flags and to state coats of arms.
        - Unless a state has completely ceded the right to use its TLDs to a non-sovereign entity and, thus has stopped using it, a TLD remains protected by state immunities.
        - In fact, the protection of these TLDs does not rest their economic value, but rather in that they embody state sovereignty.

2./ Safeguarding the provision of public international services

Proposal 2.1: The domain names of International Organizations are 'properties' to be protected through immunities

- The same reasons justifying the proposal that state domain names are 'property' that can be protected through immunities apply *mutatis mutandi* to the domain names of international organizations.
    - Useful inferences can be drawn from state individual practice and their adherence to Article 6 *ter* of the Paris Convention.

---

[24] https://hhockx.wordpress.com/2015/08/11/meeting-the-challenges-of-preserving-the-uk-web/.

[25] See for instance, [France] – *NML v République argentine,* Cour de cassation, première chambre civile, arrêt n° 394 du 28 mars *2013* (10-25.938); [Belgium] – *Argentine c. NML Capital Ltd.*, Cour de Cassation de Belgique, Première Chambre, ARRÊT n° c.11.0688.F du 22 novembre 2012 C.11.0688.F/19.

- However, the immunities of international organizations have some singularities:
    - Unlike state immunities that are often based upon customary international law, international organizations immunities find their legal source either in domestic law or in conventions.
    - In addition, such immunities are governed by the principle of speciality applicable to the legal capacity of international organizations.
        - Accordingly, in addition of express powers and rights that are granted to international organizations in their constitutive instruments, they can be presumed to possess powers that are necessary for the fulfillment of their functions.[26]
        - Thus, the capacity of international organizations to claim immunities may often be dependent on the necessity of the requested immunities to the fulfilment of their functions.
    - The recognition of immunity to the domain names or international organizations is to be implemented either to through the domestic law of individual state, or through international agreements, especially headquarters agreements.

Proposal 2.2: Entities administering domain names as providers of 'public international services' enjoy immunities ratione materiae with respect to these activities

- As alluded to above, the domain name system in general serve the function of an 'address book' of sorts when considering the infrastructure of the Internet.
    - From a technical standpoint, identifying a resource on the network is done through the use of IP addresses; those addresses, however, are numerical strings which are not appropriate for human use.
    - The domain name system alleviates this problem by allowing Internet users to rely on alphanumeric strings known as URLs to access these resources; the DNS basically takes the form of a list of registered domain names such as 'admin.ch', each one leading towards its related IP. Custody of the DNS master file, known as the 'root zone', is entrusted to ICANN by the NTIA through the IANA functions contract.

- The *Ben Haim and al. v. Islamic Republic of Iran and al.* raised a problem regarding the status of ICANN, as a non-profit association under California law, exercising functions that are critical to the good functioning of the current Internet system.
    - In this case, ICANN's motion to quash the writ of attachment was necessary because of its status as a non-profit law association under California law.[27]
    - As such, ICANN does not enjoy immunities before US domestic courts and tribunals.
        - Although many cooperation agreements between ICANN and other entities contain a provision safeguarding immunities that ICANN may benefit under international agreements and domestic laws,[28] I have found neither an agreement nor a domestic law granting ICANN immunities.

---

[26] *Legality of the Use by a State of Nuclear Weapons in Armed Conflict*, Advisory Opinion, I.C.J. Reports 1996, para. 25.

[27] https://www.icann.org/resources/pages/governance/articles-en.

[28] See for instance the Memorandum of Understanding between ICANN and the African Telecommunication Union; Memorandum of Understanding with the Commonwealth Telecommunication Organization.

- In the *Ben Haim* case, claiming that states' top level domain names are not attachable property avoided that ICANN could be judicially forced to make the ccTLDs at stake available for attachment.
    - ICANN's IANA functions seem to deserve special protection against domestic judicial intrusions for the stability of the well-functioning of the Internet system, especially in countries where TLDs are considered as 'state properties'.
        - However, nothing prevents another entity to create an alternate root zone service.
    - Thus, any proposal should be broad enough to cover entities which may need immunities for the protection because of the importance of their DNS functions in the maintenance of well-functioning Internet system.

- Granting immunities *ratione materiae* to entities administering TLDs has the advantage of protecting these entities from any judicial intrusion as far as their DNS functions are concerned.
    - In this context, only these functions are protected. The entity remains therefore remain justiciable before domestic courts for other purposes.
    - In practice, not all entities exercising IANAs functions are significant, either in scope or in magnitude, to justify the grant of immunities. In addition, their goal might also be different as, especially when they aim at creating a new space inside the Internet that the public authorities cannot touch.
        - Thus, the proposal excludes entities administering domain names when they have yet secured recognition as providers of 'public international service'.
        - In determining whether an entity exercising IANA functions provide a 'public international service', their objectives, as much as the importance of their activities in the maintenance of a stable and reliable internet, are factors to take into account.
    - Implementing this proposal requires that States, collectively, through an international instrument or, individually, in their domestic legislation enact a provision similar to similar to Article 14 of the Swiss Federal Law on State Immunities granting 'international bodies' providing an international public service the possibility to enjoy immunities, when 'the granting of privileges, immunities and facilities contributes substantially to the fulfilment of its mandate'.[29]

* * *

[29] https://www.admin.ch/opc/en/classified-compilation/20061778/index.html