INTERNET CASES IN EU PRIVATE INTERNATIONAL LAW—DEVELOPING A COHERENT APPROACH

TOBIAS LUTZI*

Abstract Internet communication has long been known to pose a challenge to private international law and its reliance on geographical connecting factors. This article looks at the problem from the perspective of EU private international law and argues that the way in which it has been accommodated by Regulations Brussels I, Rome I, and II conflicts with some of its central paradigms. It advances an alternative approach that would generally submit claims against information society service providers established in the EU to the jurisdiction and substantive laws of their 'country of origin' but make certain exceptions for private persons and consumers. The article argues that implementing such an approach would require little legislative change, be more faithful to the particularities of internet communication, and give greater effect to the central paradigms of EU private international law.

Keywords: centre of interests, conflict of laws, country of origin, EU private international law, internet, jurisdiction, mosaic approach.

I. INTRODUCTION

More than 20 years since the internet has become widely available to private users, scholars of private international law still debate whether it requires 'almost every concept and rule in the field to be reconsidered'[1] or constitutes nothing more than 'a complex problem of application'[2]. Today, more and more authors seem to ascribe to the view that 'there is nothing different or unique about cyberspace which warrants the modification or abandonment of

* DPhil candidate and tutor, Somerville College, University of Oxford, tobias.lutzi@law.ox.ac.uk. I am greatly indebted to Andrew Dickinson, who supervised the MPhil thesis on which this article is based and provided invaluable support and feedback throughout its development. In addition, I am very grateful to my MPhil examiners, Edwin Peel and Alex Mills, as well as the ICLQ anonymous peer reviewer and the participants at the International Law Lunch at the University of Cologne, particularly Heinz-Peter Mansel, all of whom have provided critical comments that have significantly improved this article. All mistakes remain my own.

[1] Lord Bingham, with regard to online defamation, in Collins, *The Law of Defamation and the Internet* (1st edn, OUP 2001), foreword (also quoted by Kirby J in *Dow Jones v Gutnick* [2002] HCA 56, [66]).

[2] A Mills, 'Rethinking Jurisdiction in International Law' (2004) 84 BYBIL 187, 197.

[*ICLQ* vol 66, July 2017 pp 687–721] doi:10.1017/S0020589317000240

traditional choice-of-law regimes';[3] but it remains undisputed that the particularities of internet communication are not easily accommodated by rules on jurisdiction and choice of law that mainly rely on geographical connecting factors.[4]

This is true, in particular, for the ubiquity[5] and virtuality[6] of Internet communication. The internet makes it possible for information to be transmitted almost instantaneously all around the globe by a single mouse click and for legal relationships to form without any physical element other than the parties[7] (and some negligible changes to the magnetization of a number of hard drives). It thus raises two antithetic challenges. The ubiquity of online communication causes a problematic multiplication of connections—up to a point where content is connected, by its accessibility, to every country in the world. At the same time, the virtuality of online communication leads to a scarcity of useful connecting factors—up to a point where the only links to any particular jurisdiction are the parties involved and the technical equipment they use. Where these two phenomena overlap, courts are confronted with an overwhelming amount of increasingly tenuous connections to a multitude of legal systems.

In the EU, the emergence of these phenomena has coincided with important reforms in the area of private international law,[8] yet, addressing them through specific rules of private international law has never been seriously considered.[9] Instruments of EU private international law thus do not differentiate between offline and online cases, both of which are governed by the general rules of Regulations Brussels Ia,[10] Rome I,[11] and II.[12]

[3] P Davis, 'The Defamation of Choice-of-Law in Cyberspace' (2002) 54 FedCommLJ 339, 341, 342. See O Bigos, 'Jurisdiction over Cross-Border Wrongs on the Internet' (2005) 54 ICLQ 585, 588–90, 602–3; U Kohl, *Jurisdiction and the Internet* (CUP 2007) 11–13; T Schulz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19(4) EJIL 799, 802–3; S Gössl, *Internetspezifisches Kollisionsrecht?* (Nomos 2014) 266. See also *Lucasfilm v Ainsworth* [2009] EWCA Civ 1328 [193]–[94]. *Contra* M Collins, *The Law of Defamation and the Internet* (3rd edn, OUP 2010) [3.01]; J Hörnle, 'The Jurisdictional Challenge of the Internet' in L Edwards and C Waelde (eds), *Law and the Internet* (3rd edn, Hart 2009) 121, 141, 157; D Svantesson, *Private International Law and the Internet* (2nd edn, Kluwer 2013) 52–62; F Wang, *Internet Jurisdiction and Choice of Law* (CUP 2010) 6.

[4] This is conceded, eg, by Schulz (n 3) 3–6 and Gössl (n 3) 29.

[5] ie its ability to have effects in many places at once. See M Bogdan, 'Website Accessibility as Basis for Jurisdiction under the Brussels I Regulation' (2011) 5 Masaryk University Journal of Law and Technology, 1, 3, 6–7; W Jiménez and A Lodder, 'Analyzing Approaches to Internet Jurisdiction Based on a Model of Harbors and the High Seas' (2015) 29 IRLCT 266, 268.

[6] ie its independence from physical elements and geographical places. See E Márton, *Violations of Personality Rights through the Internet* (Nomos 2016) 56; Svantesson (n 3) 37; Wang (n 3) 27–9, 266–7.

[7] Bigos (n 3) 590.

[8] For an overview see Lord Collins *et al.* (eds), *Dicey, Morris and Collins on The Conflict of Laws* (15th edn, Sweet & Maxwell 2012) [1–020]–[1–022].

[9] See also section III.E.

[10] Reg (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.

[11] Reg (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations.

[12] Reg (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations.

Attempts at specific internet regulation have, however, been made at the level of substantive harmonization. The most prominent example[13] is the e-Commerce Directive[14], which remains the EU legislator's most ambitious attempt to create an overarching framework of harmonized substantive rules for internet services.[15] Although its Article 3(2), which some considered to be a rule of private international law,[16] has meanwhile been characterized as nothing more than a substantive corrective,[17] it continues to have (at least) an indirect influence on the solution of internet cases in EU private international law.[18]

Still, the majority of problems caused by the aforementioned phenomena arise within the framework of the general rules of EU private international law. Over the last few decades, the European Court of Justice (ECJ) has had numerous opportunities to interpret these rules in light of this challenge.

In the following section (II), it will be argued that the interpretation(s) applied by the Court conflict heavily with the paradigms of EU private international law. In the light of this analysis, the article will then seek to develop an alternative, coherent approach to Internet cases that respects the particularities of internet communication and gives greater effect to these paradigms (III). This approach will then be outlined and tested (IV), before some conclusions are drawn (V).

II. THE PROBLEMATIC APPROACH OF EU PRIVATE INTERNATIONAL LAW TO INTERNET CASES

The ECJ has repeatedly reacted to the multiplication of connections to which the internet gives rise by indiscriminately giving effect to all of them, creating a mosaic of jurisdictional competences and applicable laws. It will be shown, though, that this approach conflicts with the central paradigms of EU private international law, both at the level of jurisdiction (A) and at the level of

[13] Another example is the new General Data Protection Regulation (Regulation (EU) No 2016/679), which defines its own territorial scope of application (in art 3) and contains a special rule for jurisdiction (in art 79(2)).

[14] Dir 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[15] See N Höning, 'The European Directive on e-Commerce and its Consequences on the Conflict of Laws' (2005) 5 Global Jurist Topics, art 2, 2–3; A Savin, *EU Internet Law* (Edward Elgar 2013) 29.

[16] See P Mankowski, 'Herkunftslandprinzip und deutsches Umsetzungsgesetz zur e-commerce Richtlinie' (2002) 22(4) IPRax 258. See also OGH 9 May 2012, MR 2012, 207, [1.2] (Austrian Supreme Court) (interpreting the Austrian transposition as a conflict-of-laws rule) and OGH 19 Mar 2013, GRUR Int 2013, 1163, 1166 (arguing that this interpretation cannot be upheld in light of *eDate*).

[17] Joined Cases C-509/09 and C-161/10 *eDate Advertising* and *Martinez* [2011] ECR I-10302, [59]–[68]. See also section III.D.3.

[18] See sections II.A.1 and II.B.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

choice of law (B), creating problems, in particular, for the providers of information society services[19] (C).

A. Jurisdiction

Under the Brussels Ia Regulation, jurisdiction over defendants domiciled in the EU is vested in the courts of their domicile (Article 4(1) Brussels Ia) and, if different, establishment[20] (Article 7(5) Brussels Ia). Alternatively, European defendants can be sued in the Member State(s) of the causal event and the damage[21] (in matters relating to tort, Article 7(2) Brussels Ia) and at the place of contract performance (in matters relating to a contract, Article 7(1) Brussels Ia).

In internet cases, the first three of these connecting factors (domicile, establishment, and place of causal event[22]) usually give rise to no more than evidentiary problems.

The fourth factor (place of the damage) has, however, turned out to be highly problematic. On numerous occasions, the ECJ has interpreted it as every place where internet content can be accessed (provided that the claimant alleges a violation of their rights in this Member State). Jurisdiction of these courts would, however, be limited to the damage caused in the Member State in question, creating a mosaic of competent jurisdictions (1). To attenuate the problems that this approach would cause with regard to violations of privacy and personality rights, the ECJ subsequently created an additional forum, allowing the victims of these torts to bring an action for all damages in their centre of interests (2).

Regarding the fifth factor (place of contract performance), the Court has not yet had the opportunity to specify its interpretation in an internet case involving services or goods delivered online;[23] but its inability to accommodate contracts which do not involve physical performance is likely to create problems (3).

1. The mosaic approach

The ECJ first applied the so-called mosaic approach to what is now Article7(2) Brussels Ia in its well-known decision in *Shevill*, which involved defamation in

[19] For lack of a better option, this term, as defined in art 2(a) e-Commerce Directive, will be used throughout this article to designate uses of the internet to provide services, goods, or information.

[20] Art 7(5) effectively extends art 4(1) in cases arising out of the operation of a 'branch, agency or other establishment' to the country in which the latter is situated.

[21] See Case 21/76 Bier [1976] ECR 1735, [19].

[22] In internet cases, the ECJ has repeatedly considered the place of the causal event to be identical with the place of domicile (or establishment) of an information society service provider (see Cases C-441/13 *Hejduk* ECLI:EU:C:2015:28, [23]–[26]; C-360/12 *Coty Germany* ECLI:EU:C:2014:1318, [49]–[52]; C-523/10 *Wintersteiger* ECLI:EU:C:2012:220, [34]–[38]; *eDate* (n 17) [42]–[43]).

[23] As opposed to cases concerning contracts that have been concluded online but still involve physical performance (as to which see, eg, Case C-322/14 *El Majdoub* ECLI:EU:C:2015:334; Joined Cases C-585/08 and C-144/09 *Pammer* and *Hotel Alpenhof* [2010] ECR I-12570).

a printed newspaper. The Court allowed the claimant to bring an action in every Member State in which the defamatory material had been distributed and in which the defendant claimed to have suffered injury to their reputation, with jurisdiction being limited to the damage caused in this Member State.[24]

Applied to online cases, this approach allows the claimant to seise the courts of every Member State in which the online content in question can be accessed,[25] provided that the right in question is protected and has allegedly been infringed there, with jurisdiction of these courts being limited to the damage caused within this Member State. The Court has so far applied it to online violations of privacy and personality rights,[26] trademarks (which are only protected in the Member State in which they have been registered),[27] copyrights (which are protected in all Member States, albeit with distinct territorial scopes[28]),[29] and unfair competition law.[30] It can presumably be extended to the violation of other territorially protected[31] IP rights.[32]

The mosaic not only raises conceptual questions, especially when contrasted to the centre-of-interests approach chosen in *eDate*.[33] Much more importantly, it has always given rise to considerable practical problems, which were certain to be amplified if it were extended to internet cases based on the mere accessibility of online content.[34]

For the *claimant*, the mosaic approach regularly makes it impossible to get compensation for their entire damage anywhere other than at the defendant's domicile (or, if applicable, place of establishment).[35] If they want to avoid the courts in this country and take advantage of the rules of special jurisdiction, they need to bring actions in up to 27 other Member States to get (almost) full compensation.[36]

[24] Case C-68/93 *Shevill* [1995] ECR I-415, [29]–[30].

[25] See *Hejduk* (n 22) [34]; Case C-170/12 *Pinckney* ECLI:EU:C:2013:635, [44].

[26] *eDate* (n 17) [42]–[44], [51].

[27] *Wintersteiger* (n 22) [28]. See also OGH 10 July 2012, GRUR Int 2013, 59, 61.

[28] By virtue of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

[29] *Hejduk* (n 22) [27]–[37]; *Pinckney* (n 25) [43]–[46]. See also Case C-387/12 *Hi Hotel* ECLI:EU:C:2014:215, [35]–[39], for a case of offline infringement.

[30] Case C-618/15 *Concurrence SARL* ECLI:EU:C:2016:976, [31]–[34]; *Coty Germany* (n 22) [55]–[57].

[31] As opposed to uniform IP rights, which are governed by specific EU instruments such as Regulation (EC) 207/2009 on the Community trade mark.

[32] P Stone, 'Territorial Targeting in EU Private Law' (2013) 22 Info&CommTechL 14, 22–3.

[33] See section II.A.2.

[34] See E Lein in A Dickinson and E Lein (eds), *The Brussels I Regulation Recast* (OUP 2015) [4.112]; B Hess 'The Protection of Privacy in the Case Law of the CJEU' in B Hess and C Mariottini (eds), *Protecting Privacy in Private International and Procedural Law by Data Protection* (Nomos 2015) 89–90; J Oster 'Rethinking *Shevill*. Conceptualising the EU Private International Law of Internet Torts against Personality Rights' (2012) 26 IntRevLCompTech, 113, 116–17.

[35] See above, at (n 22).

[36] Martón (n 6) 181–2; M Šrámek, 'Brussels I: Recent Developments in the Interpretation of Special Jurisdiction Provisions for Internet Torts' (2015) 9 Masaryk University Journal of Law

For the *defendant*, it creates the (theoretical) risk of being sued in up to 28 Member States,[37] which makes it prohibitively burdensome to defend these actions even where the claimant's case is very weak. The limitation of individual actions to a small portion of the damage will often do little to decrease this risk given that even a tiny fraction of the overall damage can result in an award of considerable damages (plus costs).[38] Moreover, even a small fraction of the damage suffered in one country can be used to seek an injunction from its courts, which, in practice, may often require the defendant to stop the activity in question altogether,[39] given that many online activities have ubiquitous effects and cannot easily be territorially limited.[40]

Thus, for the *courts*, the mosaic approach raises the question whether they should grant an injunction based on their jurisdiction for only a small portion of the overall damage in these circumstances.[41] The English courts, for instance, have generally been hesitant to issue injunctions against online publications of defamatory content where their jurisdiction was based on only a part of the overall publication having been accessed in England.[42] German courts, on the other hand, have always been willing to grant injunctions, their jurisdiction generally being assumed for the entirety of the damage caused by the action complained of.[43] The ECJ, meanwhile, was confronted with the question in *eDate*[44] but ultimately did not need to address it as jurisdiction of the referring court for the entirety of the claim could be based on the centre-of-interests approach.[45] The question has now been referred to the Court again.[46]

and Technology 165, 171; K Kreuzer and P Klötgen 'Die Shevill-Entscheidung des EuGH' IPRax (1997) 90, 96.

[37] AG Cruz Villalón, Opinion on Case C-441/13 *Hejduk* ECLI:EU:C:2014:2212, [43]; Lein (n 34) [4.112]; Oster (n 34) 116; Stone (n 32) 17; S Bollée and B Haftel, 'Les nouveaux (dés) équilibres de la compétence internationale en matière de cyberdélits après l'arrêt eDate Advertising et Martinez' Dalloz (2012) 1285, 1292.

[38] See *Bin Mahfouz v Ehrenfeld* [2005] EWHC 1156 (QB), where the defendant was ordered to pay £115,000 over 23 copies of her allegedly defamatory book that were sold in England and the first chapter that was made available online. See also T Hartley, '"Libel Tourism" and Conflict of Laws' (2010) 59 ICLQ 25, 31–2; M Reymond, 'The ECJ *eDate* Decision: A Case Comment' (2011) 13 YrbkPrivIntlL 493, 503.

[39] Bogdan (n 5) 5; Hartley (n 38) 31–2; Hess (n 34) 90, 106; Schulz (n 3) 814–16.

[40] See, in more detail, section III.A.

[41] It has been argued by Bigos (n 3) 617–18, and Bogdan (n 5) 5, that this question can be solved by the courts exercising the discretion they enjoy under the applicable procedural law; yet, not only does this presuppose that all national laws provide for such a discretion (which they do not), it also does not answer the question whether courts should have the competence to issue an injunction in these cases. The recent decision by the UK Supreme Court to uphold an injunction against publication of certain information in England although it had already been widely disseminated over the internet (*PJS v News Group Newspapers* [2016] UKSC 26, [2016] AC 1081) illustrates the pertinence of this question.

[42] *King v Lewis* [2004] EWCA Civ 1329, [2005] ILPr 16, [2]; but see *Jameel (Yousef) v Dow Jones* [2005] EWCA Civ 75, [2005] QB 946, [72]–[74].

[43] See, eg, OLG Düsseldorf 22 June 2011, IPRspr 2011, Nr 237, 611 (Higher Regional Court Düsseldorf; following BGH 2 March 2010, *New York Times*, BGHZ 184, 313 (German Federal Court of Justice)).

[44] *eDate* (n 17) [24].

[45] For which see section II.A.2.

[46] Case C-194/16 *Bolagsupplysningen* OJ C 211 (13 June 2016) 35, question 1.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

Still, even where the claimant only seeks monetary compensation, the courts face a considerable challenge in quantifying which part of the damage has been caused by the accessibility of the content in their jurisdiction.[47]

By creating dozens of potential fora, the mosaic approach thus gives a significant jurisdictional advantage to potential claimants. While one may consider this to be justified by the wish to protect the rights of the victims of personality and IP right infringements,[48] it obviously comes at the price of exposing potential defendants to the risk of being easily sued everywhere in the EU. Besides, this justification seems at odds with the ECJ's position that the special ground for jurisdiction in Article 7(2) Brussels Ia does not serve the purpose of protecting the weaker party.[49]

Moreover, the mosaic approach conflicts with several central paradigms of EU private international law.

The fact that claimants can pick from a wide range of jurisdictions, for instance, makes it almost impossible for defendants to foresee in which of the Member States where the online content in question is available they may be sued.[50] This directly conflicts[51] with the *principle of legal certainty*[52] which, according to the ECJ,

> requires, in particular, that the jurisdictional rules which derogate from the basic principle of [the Brussels Ia Regulation] laid down in [Article 4], such as the rule in [Article 7(1)], should be interpreted in such a way as to enable a normally well-informed defendant reasonably to foresee before which courts, other than those of the State in which he is domiciled, he may be sued.[53]

[47] AG Cruz Villalón, Opinion on *Hejduk* (n 37) [20], [39]–[40]; Hess (n 34) 90, 98, 106; Lein (n 34) [4.112]; Martón (n 6) 177–78; Šrámek (n 36) 171; Stone (n 32) 17.

[48] See, to this effect, AG Cruz Villalón, Opinion on Joined Cases C-509/09 and C-161/10 *eDate Advertising* and *Martinez* [2011] ECR I-10302, [48].

[49] See Cases C-45/13 *Kainz* ECLI:EU:C:2014:7, [31]; C-133/11 *Folien Fischer* ECLI:EU:C:2012:664, [46].

[50] AG Cruz Villalón, Opinion on *Hejduk* (n 37) [43]; AG Jääskinen, Opinion on Case C-170/12 *Pinckney* ECLI:EU:C:2013:400, [68]; A Thünken, 'Multi-State Advertising over the Internet and the Private International Law of Unfair Competition' (2002) 51 ICLQ 909, 933; T Pfeiffer in B Hess, T Pfeiffer and P Schlosser (eds), *The Brussels I Regulation* (Beck 2008) [203]. Schulz (n 3) 813–14, argues that this is not a major problem since defendants only need to worry about jurisdictions where decisions can be enforced; still, for EU-based defendants, this is at least every single Member State of the EU.

[51] Schulz (n 3) 815; P Picht, 'Von eDate zu Wintersteiger' GRUR Int (2013) 19, 23.

[52] See generally A Dickinson, 'Legal Certainty and the Brussels Convention – Too Much of a Good Thing?' in P de Vareilles-Sommières (ed), *Forum Shopping in the European Judicial Area* (Hart 2007) 115.

[53] Case C-256/00 *Besix* [2002] ECR I-1718, [26]. See also Cases C-440/97 *Groupe Concorde* [1999] ECR I-6307, [24]; C-26/91 *Handte* [1992] ECR I-3967, [18].

It also conflicts with the 'fundamental'[54] principle of *actor sequitur forum rei*[55] as it regularly offers the claimant a wide range of alternative fora, usually including their own home country.[56]

By the same token, the mosaic approach conflicts with the *principle of proximity*[57] as it allows for jurisdiction to be based on the very tenuous connection between the forum and the content being accessible there,[58] although 'it is that connection which justifies the special jurisdiction provided for in [Article 7(2) Brussels Ia]'.[59] Not only is this highly problematic where it is used to obtain an injunction prohibiting publication of the content in question altogether,[60] it also has a considerable potential to increase forum shopping within the EU.[61] For instance, it is widely believed that the easy availability of the English courts in cases of online defamation[62] has created 'libel tourism' in England.[63] This risk appears to be even bigger under the Brussels Ia Regulation,[64] the broad grounds for jurisdiction of which are not balanced out by any judicial discretion.[65]

Finally, the mosaic approach conflicts with the *principle of sound administration of justice*,[66] according to which 'it is necessary to avoid the

[54] *Coty Germany* (n 22) [44]; *Besix* (n 53) [53].

[55] See Cases C-412/98 *Group Josi* [2000] ECR I-5925, [34]–[35]; *Handte* (n 53) [14]; H van Lith in Dickinson and Lein (n 34) [3.04]; M Lehmann ibid [4.07].

[56] Oster (n 34) 117. See also *Besix* (n 53) [54]. Based on the mosaic approach, the claimants were allowed to sue in their home courts in *Wintersteiger* (n 22), *Pinckney* (n 25), *Hejduk* (n 22), *Coty* (n 22), and *Concurrence SARL* (n 31).

[57] See generally E Lein, 'The New Rome I/Rome II/Brussels I Synergy' (2008) 10 YrbkPrivIntlL 177.

[58] AG Cruz Villalón, Opinion on *Hejduk* (n 37) [44]; AG Jääskinen, Opinion on *Pinckney* (n 50) [69]; Picht (n 51) 23.

[59] Case C-364/93 *Marinari* [1995] ECR I-2719, [20]. See also Cases C-12/15 *Universal Music* ECLI:EU:C:2016:449, [27]; 56/79 *Zelger (No 1)* [1980] ECR 89, [3].

[60] See above, at n 41.

[61] AG Jääskinen, Opinion on *Pinckney* (n 50) [68]; Hess (n 34) 106; Hörnle (n 3) 137–8; B Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IntJLInfoTech 142, 50; Martón (n 6) 185–7; Oster (n 34) 117. See also, by analogy, *Besix* (n 53) [34].

[62] See, in particular, *Berezovsky v Forbes* [2000] 1 WLR 1004 (UKHL) and *King v Lewis* (n 42). This availability seems to have ended with section 9 of the 2013 Defamation Act.

[63] See Hartley (n 38) 26–7, 30; C Mariottini, 'Freedom of Speech and Foreign Defamation Judgments' in Hess and Mariottini (n 34) 115, 138–46; A Mills, 'The Law Applicable to Cross-Border Defamation on Social Media: Whose Law Governs Free Speech in "Facebookistan"?' [2015] JMediaL 1, 3–6; Reymond (n 38) 494; Bollée and Haftel (n 37) 1292.

[64] Hörnle (n 3) 139–40; Mills (n 63) 6.

[65] See Case C-281/02 *Owusu* [2005] ECR I-1383. The English courts, on the other hand, could set aside proceedings where the claim based on accessibility of content in England amounted to an abuse of process (see *Jameel v Dow Jones* (n 43) [50]–[77]; *Lonzim v Sprague* [2009] EWHC 2838 (QB); *Kaschke v Osler* [2010] EWHC 1075 (QB); *Subotic v Knezevic* [2013] EWHC 3011 (QB); *Karpov v Browder* [2013] EWHC 3071 (QB); but see also *Mardas v New York Times* [2008] EWHC 3135 (QB), where a plea for *forum non conveniens* remained unsuccessful as 177 printed copies published in England were considered as 'real and substantial' and it was said that 'a few dozen [people who have accessed an online article] is enough to found a cause of action here' (ibid [25], [31]).

[66] AG Cruz Villalón, Opinion on *eDate* (n 48) [51]; Opinion on *Hejduk* (n 37) [42]; AG Jääskinen, Opinion on *Pinckney* (n 50) [68]. See also Martón (n 6) 98–100.

multiplication of courts of competent jurisdiction which would heighten the risk of irreconcilable decisions […]'.[67] The mosaic approach risks creating a multiplicity of lawsuits that have essentially the same object.[68] This is as burdensome for the parties, who may have to bring or defend these multiple actions—which will always benefit the stronger party, who has the necessary resources to do so[69]—as it is for the courts of the Member States. It has been claimed that they may remedy this problem by granting stays where a similar action is pending in the courts of another Member State.[70] Yet, as each of these actions will technically have a different object (ie the damage caused within that particular jurisdiction), such a stay could only be based on Article 30(1) Brussels Ia. Article 30(1) gives the courts discretion to stay proceedings in order to prevent irreconcilable decisions[71] but still requires them to adjudicate eventually, once the action pending elsewhere has been decided. A court may only *decline* jurisdiction (under Article 30(2)) if the court seized with a related action will be able to hear both actions together, which will not be the case if its jurisdiction is territorially limited under the mosaic approach.

From the defendant's point of view, some of these problems may appear to be balanced out, at the level of choice of law, by the e-Commerce Directive. The country-of-origin principle in its Article 3(2) exempts the defendant, in its 'coordinated field', from having to comply with the substantive laws of multiple Member States even where they are subject to the jurisdiction of the courts in these States. However, it does not reduce the procedural burden of having to defend an action in each of these Member States.

2. *The centre of interests*

In light of 'the serious nature of the harm which may be suffered by the holder of a personality right who establishes that information injurious to that right is available on a world-wide basis',[72] the ECJ tried to remedy the aforementioned difficulties for the claimant by allowing them to bring an action for the entire damage at their 'centre of interests'. This approach has rightly been criticized for a number of reasons.[73]

First, it is unclear whether the Court understands the centre of interests as a manifestation of the place of the damage or as an independent ground for jurisdiction.[74] The first understanding seems difficult to reconcile with the mosaic approach, according to which damage is suffered in every Member

[67] C-220/88 *Dumez France* [1990] ECR I-49, [17]–[18]. See also *Besix* (n 53) [27]; Case 266/85 *Shenavai* [1987] ECR 239, [8].
[68] Martón (n 6) 175, 190–5; Picht (n 51) 23.
[69] *Contra* Bigos (n 3) 611.
[70] Bigos (n 3) 610.
[71] See recital (21) Brussels Ia.
[72] *eDate* (n 17) [47]; see also AG Cruz Villalón, Opinion on *eDate* (n 48) [48].
[73] See, eg, Mills (n 63) 20–1; Hess (n 34) 93–4; 94–5, 106; Reymond (n 38) 498–503; S Schmitz, 'From Where Are They Casting Stones? – Determining Jurisdiction in Online Defamation Claims' (2012) 6 Masaryk UJLTech 159, 173–5; Bollée and Haftel (n 37) 1286–90. More positive: Lein (n 34) [4.120]; Oster (n 34) 120–2.
[74] The wording of eDate (n 17) [51], seems to indicate that it is a separate ground for jurisdiction.

State where internet content is accessible and which the ECJ expressly upheld in *eDate*;[75] the second understanding raises important questions as to the legal basis of this new ground for jurisdiction.[76]

Second, the centre-of-interest approach further undermines the principle of *actor sequitur forum* by allowing the claimant to bring an action for the entire damage in what will normally be their home jurisdiction.[77] The ECJ thus created a *forum actoris*,[78] although '[a]part from the cases expressly provided for, the [Brussels Ia Regulation] does not appear to favour the attribution of jurisdiction to the courts of the claimant's domicile'.[79] This further disadvantages the defendant, who already bears the lion's share of the burden created by the mosaic approach.[80]

Third, it requires some difficult distinctions in practice. On the one hand, violations of personality rights need to be satisfactorily distinguished from other rights, the protection of which is strictly territorial.[81] On the other hand, online infringements need to be distinguished from other (offline) forms of personality right violations, where 'the nature of the harm' is not 'serious' enough to justify the attribution of jurisdiction for the entire damage to the courts at the claimant's centre of interests.[82] Yet, online and offline activity are rapidly converging,[83] making such a distinction more and more difficult.[84]

Finally, although the ECJ justified its solution by an expected increase in legal certainty,[85] it may not always be clear where a person has their centre of interests,[86] as can be seen from the questions recently referred to the Court in *Bolagsupplysningen*.[87]

3. *The place of contract performance*

A separate but not entirely unrelated problem arises with regard to the connecting factor used in Article 7(1) Brussels Ia, which vests special jurisdiction in the courts of the place of contract performance. The mere fact

[75] Martón (n 6) 176; Reymond (n 38) 499–501; Bollée and Haftel (n 37) 1287–8.
[76] Bollée and Haftel (n 37) 1287: 'un excès de pouvoir de la part de la CJUE'.
[77] ibid. See also BGH 2 March 2010, *New York Times* (n 43) [17].
[78] AG Cruz Villalón, Opinion on *Hejduk* (n 37) [26]; AG Jääskinen, Opinion on *Pinckney* (n 50) [69]; Martón (n 6) 263; Bollée and Haftel (n 37) 1286; Picht (n 51) 22.
[79] Case C-464/01 *Gruber* [2005] ECR I-472, [33]. See also Cases C-168/02 *Kronhofer* [2004] ECR I-6009, [20]; C-269/95 *Benincasa* [1997] ECR I-3767, [14]; C-89/91 *Shearson Lehman Hutton* [1993] ECR I-139, [17]; C-220/88 *Dumez France* [1990] ECR I-49, [19].
[80] Bollée and Haftel (n 37) 1288–9; Picht (n 51) 22.
[81] Bogdan (n 5) 200; Bollée and Haftel (n 37) 1289.
[82] Mills (n 63) 21; Bollée and Haftel (n 37) 1291.
[83] See M Thelwall, 'Society on the Web' in W Dutton (ed), *The Oxford Handbook of Internet Studies* (OUP 2013) 69–70.
[84] Martón (n 6) 295–8; Svantesson (n 3) 50–1; D Svantesson, 'The Holy Trinity of Legal Fictions Undermining the Application of Law to the Global Internet' (2015) 23 IntJLInfoTech 219, 220.
[85] *eDate* (n 17) [50].
[86] Hess (n 34) 93–4; Mills (n 63) 21; Bollée/Haftel (n 38) 1289.
[87] *Bolagsupplysningen* (n 46) questions 2 and 3.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

that a contract has been concluded online does not make it more difficult to determine this place; but the fact that the internet allows for contracts that do not involve any form of physical performance does.[88] For sales of digital content like music files or software, online services like the provision of storage space, cloud services,[89] or access to a streaming platform, or contracts concluded within virtual environments,[90] identifying a distinct place of performance may often be very difficult, if not impossible.

As most of these contracts contain jurisdiction clauses,[91] the ECJ has not yet had the opportunity to interpret Article 7(1) Brussels Ia in such a case. Instead, the Court has defined the place of performance in light of contracts involving physical performance,[92] holding that it would be the place where the relevant obligation is principally performed,[93] ascertained independently of the applicable law.[94] Analogies to contracts that do not involve physical performance have to be drawn with great care.

Contracts for the sale of goods, for instance, have been held to be performed at 'the place where the goods were physically transferred or should have been physically transferred' to the buyer.[95] Yet, to follow this reasoning and consider the place where the buyer downloads an e-book or a music file as the place of performance would conflict severely with the principles of legal certainty and proximity that underlie the ECJ's decision:[96] neither is it possible to predict where content will be downloaded or accessed[97] nor will it necessarily establish the required 'close link between the contract and the court called upon to hear and determine the case'[98]. As alternatives, one might consider the buyer's domicile[99] (which would however undermine the principle of

[88] Foss/Bygrave, 'International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law' (2000) 8(2) IntJLInfoTech 99, 108; Wang (n 3) 52–3: 'digitized products'. See also Hörnle (n 3) 126; Svantesson (n 3) 331–2; and above, at n 23.

[89] As to which, see G Haibach, 'Cloud Computing and European Union Private International Law' (2015) 11(2) JPrivIntL 252, who (correctly) qualifies (most) cloud services as service contracts (at 260).

[90] As to which, see T Lutzi, 'Aktuelle Rechtsfragen zum Handel mit virtuellen Gegenständen in Computerspielen' NJW (2012) 2070.

[91] Savin (n 15) 60; Haibach (n 89) 256, 259, 266; Wang (n 3) 19. For the problems these clauses raise, see, eg, *El Majdoub* (n 23); BGH 30 Mar 2006, BGHZ 167, 83; 24 Apr 2013, RIW 2013, 563. See also A Dickinson and J Ungerer, '"Click Wrapping" Choice of Court Agreements in the Brussels I Regime' [2016] LMCLQ 15.

[92] While Case C-533/07 *Falco Privatstiftung* [2009] ECR I-03327 involved a non-physical object (IP rights), the court did not qualify it as a service contract; consequently, it only needed to discuss the place of performance of the 'obligation in question' under art 7(1)(a) Brussels Ia, ie the obligation of payment (see ibid [47]).

[93] Cases C-386/05 *Color Drack* [2007] ECR I-03699, [40]; C-19/09 *Wood Floor* [2010] ECR I-2121, [40].

[94] Case C-381/08 *Car Trim* [2010] ECR I-01255, [52]–[53], overruling Case 12/76, *Tessili* [1976] ECR 1473.

[95] *Car Trim* (n 94) [60].

[96] See ibid [48]–[49], [61].

[97] Wang (n 3) 54, 56.

[98] *Color Drack* (n 93) [22]; *Wood Floor* (n 93) [22].

[99] Wang (n 3) 56–7.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

actor sequitur forum) or the seller's domicile[100] (which would however frequently yield the same result as Article 4(1) Brussels Ia) as the place of performance; but neither appears wholly satisfactory.

By the same token, the place of performance of a contract for the provision of web space or cloud services is not likely to be the place where the service is accessed. Instead, one may have to look at the domicile of the recipient[101] or the place from where the data is administered.[102] The latter would be in line with the ECJ's decision in *Wood Floor*[103] and the principle of proximity but would, again, often make no difference to Article 4(1) Brussels Ia.

B. Choice of Law

Similar problems exist at the level of choice of law.

Just as with the place-of-the-damage limb of Article 7(2) Brussels Ia, several provisions of the Rome II Regulation give rise to a mosaic of applicable laws. This is true for Article 8(1) Rome II, which submits violations of territorially protected IP rights to the *lex loci protectionis* (ie the law(s) of the Member State(s) for which the claimant seeks protection)[104] as well as Article 6(3) Rome II, which refers acts of unfair competition to the law of the Member State in which competitive relations or consumer interests are affected (and which the ECJ has recently interpreted as the Member State(s) to which an online activity is directed) [105]. Similarly, the national choice-of-law rules for violations of personality rights[106] of many Member States follow the mosaic approach and require a competent court to apply several laws cumulatively.[107]

From the point of view of a potential defendant, this creates a problematic overlap of numerous applicable laws that govern a single activity. It is thus subject to the same criticism as the mosaic approach to jurisdiction as it conflicts with both the principle of legal certainty (by making it hard to foresee which laws have to be complied with) and the principle of proximity (by factually submitting defendants to the most restrictive law, even where this is not particularly closely related to the case at hand).[108] According to

[100] G-A Droz and H Gaudemet-Tallon, 'La transformation de la Convention de Bruxelles du 27 septembre 1968 en Reglèment' (2001) Rev crit DIP 601, 636; P Gottwald, in W Krüger and T Rauscher (eds), *Münchener Kommentar zur ZPO* (4th edn, Beck 2013) [27].

[101] Wang (n 3) 56–7.

[102] Haibach (n 89) 261.

[103] *Wood Floor* (n 93) [42].

[104] See A Dickinson, *The Rome II Regulation* (OUP 2008) [8.25]–[8.26].

[105] Case C-191/15 *Verein für Konsumenteninformation (VKI)* ECLI:EU:C:2016:612, [43].

[106] Which still apply as a result of the exclusion in art 1(2)(g) Rome II.

[107] See, eg, *Berezovsky v Forbes* [2000] 1 WLR 1004 (UKHL) 1012–1013, for the English common law; OLG Hamburg 8 Dec 1994, NJW-RR 1995, 790, 792, for German law. See also MainStrat, 'Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality' JLS/2007/C4/028, Final Report, 77–112, for a general overview.

[108] Pfeiffer (n 51) [203]; Svantesson (n 84) 228–9; D Svantesson, 'Between a Rock and a Hard Place – An International Law Perspective of the Difficult Position of Globally Active Internet Intermediaries' (2014) 30 CompLSecRev 348, 349; N Dethloff, 'Marketing im Internet und

some authors, the wealth of applicable laws puts the providers of information society services in a situation where they will ultimately have to decide themselves which substantive laws to comply with, based on their respective risk of enforcement.[109]

For information society service providers that are established in the EU, these problems are alleviated by the country-of-origin principle of Article 3(2) e-Commerce Directive, which exempts them from compliance with all laws that are more restrictive than the respective substantive laws of their home country.[110] Yet, the principle does not apply in the area of IP law (even though the *lex loci protectionis* rule is particularly likely to create an overlap between potentially applicable laws). Moreover, it requires the courts, in each case, to draw a comparison between the regulatory burden imposed by the law that would apply following the relevant choice-of-law rules and the law of the defendant's country of origin—an exercise that is onerous, increases costs and reduces the legal certainty that the e-Commerce Directive aims to provide.

C. Conclusion

Overall, the answers given by EU private international law to the challenges posed by the ubiquity and virtuality of internet communication conflict with several of its fundamental principles. They raise considerable problems for the providers of information society services, who face a risk of being sued in every single EU Member State and have to comply, outside the scope of application of the e-Commerce Directive, with numerous overlapping national laws.

As a consequence, in the following sections of this article, an attempt will be made at developing an approach to internet cases that addresses, in particular, the concerns of information society service providers by giving greater weight to both the particularities of internet communication and the paradigms of EU private international law.

III. DEVELOPING A COHERENT APPROACH TO INTERNET CASES

A coherent approach to internet cases that addresses the aforementioned problems has to take into account the role the internet plays in today's society and economy (A.), the interests of the parties who use it (B.), the general problem of localization to which it gives rise (C.), the different solutions that have been proposed (D.), and the different ways in which they could be implemented (E.).

Internationales Wettbewerbsrecht' NJW (1998) 1596, 1601–2. See also AG Jääskinen, Opinion on *Pinckney* (n 50) [68]. Note that neither art 6 nor art 8 Rome II contain an escape clause.

[109] Reed, *Making Laws for Cyberspace* (OUP 2012) 15; Schulz (n 3) 813–14; Svantesson (n 84) 228–30; Svantesson (n 108) 349–50, 353.

[110] See *eDate* (n 17) [64]–[68].

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

A. Use of the Internet Today

The mosaic approach to jurisdiction and choice of law and the resulting multiplication of fora and applicable laws are often justified by the idea that someone who distributes content via the internet or offers a service online does so in order to reach a worldwide audience.[111] Therefore, it is argued, they have no reason to complain about being subject to the jurisdiction of courts and the application of substantive laws from all around the globe.[112]

However, in an ever-growing number of sectors, online activity is not merely one out of many different ways to reach an audience; it virtually is the only one.[113] Even a local newspaper or a student-run campus journal is hardly read if only distributed in printed form; the same is true for the sellers of many products, especially electronic ones, and the providers of services such as transportation, accommodation, or shipping. A growing number of business models would even be outright impossible without using the internet; the list includes a wide range of activities and companies, from major players like *Google*, *Facebook*, and *Amazon* to rising start-ups like *Uber* and *AirBnB* to small blogs and not-for-profit projects like *Wikipedia* or *change.org*.

This has two important consequences. First, there is an unprecedentedly wide range of people and entities that use the internet to provide services, goods or information to users; and many of them will not be professionals.[114] Second, the mere fact that someone uses the internet does not evidence an intention to target a worldwide audience.[115]

Of course, in some cases, it is possible to restrict publications and other online services to certain jurisdictions. This is true, in particular, for services that are based on some form of subscription or registration[116] or involve the delivery of physical goods, which will usually require provision of an actual address or a bank account in a certain country. Yet, these restrictions can easily be circumvented by using a fake address or signing up under the name of a different person. Moreover, they would seriously undermine many of the aforementioned business models, which rely on a low threshold of access. Services built on the dissemination and easy availability of information like *Twitter* or *Wikipedia*, for instance, would not have been the success stories they were, had their content not been freely accessible without registration. Similarly, newspapers that have limited access to their online content to

[111] See, eg, *eDate* (n 17) [45]; *Gutnick* (n 1) [19], [39], [181]; *King v Lewis* (n 43) [29], [33]–[34]; Bigos (n 3) 612; Höning (n 15) 30; Schulz (n 3) 820.
[112] *Dicey, Morris and Collins* (n 8) [31–119]; Oster (n 34) 116; Svantesson (n 108) 350.
[113] Hörnle (n 3) 134; Martón (n 6) 64–5; Oster (n 34) 116.
[114] Martón (n 6) 65, 67–68; Reymond (n 38) 498; M Reymond, 'Jurisdiction in Case of Personality Torts Committed over the Internet' (2012/13) 14 YrbkPrivIntlL 205, 210–11.
[115] See *Pammer* (n 23) [68].
[116] Bigos (n 3) 603; Schulz (n 3) 820.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

registered (paying) users have often seen a stark decline in readership, which has sometimes even forced them to reverse the decision.[117]

Where registration of users is not an option, information society service providers may also try to restrict their content geographically by use of geo-blocking technology.[118] However, such technology is not only notoriously imperfect,[119] it also creates serious obstacles to the common market when applied within the EU. Consequently, it is vehemently opposed by the EU Commission.[120] Moreover, it is, again, irreconcilable with certain business models, especially those that rely on the participation of a big international user base, such as social networks like *Facebook*, online encyclopedias like *Wikipedia*, or review websites like *TripAdvisor*.

As a consequence, the mosaic approach to jurisdiction and choice of law often leaves information society service providers that are unable to defend lawsuits in every jurisdiction and to comply with every substantive law that may potentially apply to their activity with a very unfortunate choice: to selectively comply with the laws that are most likely to be enforced and otherwise accept the risk of liability,[121] or to cease their activity altogether.

B. Interests to Consider

In order to properly accommodate this reality within private international law, it is important to be aware of the different interests involved.

For the providers of information society services, it is desirable to be subject to a limited number of jurisdictions and applicable laws even where their content is accessible worldwide.[122] This is particularly true for service providers that do not act in a professional capacity.

[117] See, eg, M Sweney, 'Sun Website to Scrap Paywall' (30 Oct 2015) <https://www.theguardian.com/media/2015/oct/30/sun-website-to-scrap-paywall>.

[118] For arguments in favour of geo-blocking, see G Mazziotti, 'Is Geo-Blocking a Real Cause for Concern in Europe?' [2016] EIPR 365, 368–71, 372–75; Schulz (n 3) 819; Svantesson (n 3) 435–40; 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 CompLSecRep 298, 303; D Svantesson, 'Time for the Law to Take Internet Geo-location Technologies Seriously' (2012) 8(3) JPrivInyL 473.

[119] Martón (n 6) 60–62; Mazziotti (n 118) 366; Bogdan (n 5) 5; Schulz (n 3) 820–1. But see Svantesson (n 3) 400–18.

[120] See, in particular, the Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Reg (EC) No 2006/2004 and Dir 2009/22/EC, COM(2016) 289 final. See also EU Digital Single Market Strategy, COM (2015) 192 final, 6; Art 20(2) Directive 2006/123/EC. Both the Commission and the ECJ also try to fight geo-blocking by means of competition law (see EU Commission (Press Release), 'Antitrust: Commission investigates restrictions affecting cross border provision of pay TV services' (13 Jan 2014) <http://europa.eu/rapid/press-release_IP-14-15_en.htm>; Joined Cases C-403/08 and C-429/08 *Premier League and Karen Murphy* [2011] ECR I-9083.

[121] See section II.B.

[122] See Šrámek (n 37) 166; Martón (n 6) 67–8; Wang (n 3) 19; T Lutzi, '"Cross-border Defamation" auf Wikipedia' RIW (2014) 810, 813.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

The users of these services and other potential claimants (IP right holders, competitors), on the other hand, are interested in a high level of protection under laws that are accessible to them and provided, ideally, by local courts.[123]

From the regulatory point of view of the EU, finally, it is important to give effect, in principle, to both of these interests. The EU has an obvious interest in reducing the overlap of jurisdictions and applicable laws created by the mosaic approach, in particular within the common market, in order to further legal certainty, the sound administration of justice, the provision of information society services to users in all 28 Member States, and compliance with the substantive laws of the Member States.[124] In principle, this could be achieved by vesting jurisdiction in a small number of courts that are particularly closely connected to the dispute and rendering a single law applicable to a given online activity—an approach that seems to be well in line with EU private international law's function to allocate judicial and regulatory competences between the Member States.[125]

Yet, the EU's interest in stimulating the common market for information society services needs to be balanced with the need to provide adequate protection to EU citizens. In the area of contract law, this achieved by the privileges awarded to structurally weaker parties in Article 10–23 Brussels Ia and Article 5–8 Rome I, which do not have an equivalent in tort law.

C. The Problem of Localization

Many of the problems in giving effect to these competing interests in internet cases ultimately come down to a problem of localization. Leading to a multiplication of increasingly tenuous connections to any physical place, the ubiquity and virtuality of internet communication make it very hard, and, in some cases entirely impossible, to apply connecting factors that rely on the geographical localization of certain events such as 'the place of the damage', 'the affected market', or 'the place of contract performance'.[126]

In contrast, connecting factors that focus exclusively on the defendant, including the place where they acted, are not subject to these problems as they usually only point to a single or, at worst, a small number of places that usually are easy to identify.[127]

[123] See Šrámek (n 37) 166; Wang (n 3) 19.

[124] See EU Digital Single Market Strategy (n 120) 4–5.

[125] A Mills, 'Variable Geometry, Peer Governance, and the Public International Perspective on Private International Law' in H Muir Watt and D Fernández Arroyo (eds), *Private International Law and Global Governance* (OUP 2014) 250–1; H Muir Watt, 'The Role of the Conflict of Laws in European Private Law' in C Twigg-Flesner (ed), *The Cambridge Companion to European Union Private Law* (CUP 2010) 44, 46–8.

[126] See AG Cruz Villalón, Opinion on *Hejduk* (n 37) [41]–[45].

[127] AG Cruz Villalón, Opinion on *Hejduk* (n 37) [41];C Beall, 'The Scientological Defenestration of Choice-of-Law Doctrines for Publication Torts on the Internet' (1997) 15 John

D. Potential Ways of Concentration

Thus, it has been repeatedly proposed to counter the aforementioned multiplication of tenuous connections and the resulting fragmentation of jurisdiction and applicable laws by using connecting factors that allow for some form of concentration or focalization. The most prominent examples are the place of the server (1.), the claimant's centre of interests (2.), the place targeted by the information society service in question (3.), and the country from where the service is provided (4.).

1. Place of the server

One of the earliest forms of concentration that has been proposed is the place of the server where the activity in question technically takes place.[128] In light of the difficulty of identifying this place and its risk of being manipulated, the ECJ has, however, made clear that it is unsuitable as a connecting factor[129] and it seems to have long lost any support.[130]

2. Centre of interests

Another form of concentration that is occasionally proposed consists in extending the jurisdiction of the courts at the claimant's centre of interests, which the ECJ recognized in *eDate* with regard to personality right violations, to other torts.[131] Such an extension would have the advantage of making it unnecessary to distinguish between personality right violations and other torts and providing the courts with an easily identifiable criterion.

Yet, it would still be subject to the many other objections raised above.[132] Besides, it would only have a concentrating effect from the claimant's point of view; the defendant provider of online content would still be subject to the jurisdiction of the courts of all EU Member States, depending on where the individual defendant has their centre of interests.

3. Targeting

By far the most popular proposition to reduce the unwelcome effects of the mosaic theory seems to be the concept of 'targeting'. Inspired by the ECJ's

MarshallJComputer&InfoL 361, 363. See also Case C-292/10 *de Visser* ECLI:EU:C:2012:142, [37]–[42].

[128] See, eg, *Gutnick* (n 1) [20].

[129] *Wintersteiger* (n 22) [36].

[130] See Case C-173/11 *Football Dataco* ECLI:EU:C:2012:115, [44]–[46]; Bigos (n 3) 603; A Briggs, *Private International Law in English Courts* (OUP 2014) [3.156]; Hörnle (n 3) 126; Svantesson (n 3) 356–7; Gössl (n 3) 275–6. It is all the more surprising that a US District Court recently relied on it in *MacDermid, Inc v Deiter* 702 F3d 725 (2nd Cir 2012).

[131] See Hess (n 34) 106. See also the propositions made by the claimant in *Pinckney* (AG Jääskinen, Opinion on *Pinckney* (n 50) [69]) and the Czech and Swiss governments in *Hejduk* (AG Cruz Villalón, Opinion on *Hejduk* (n 37) [18]).

[132] In particular under section II.A.2.

jurisprudence on the substantive scope of several instruments of IP law[133] and Article 17(1)(c) Brussels Ia,[134] it was suggested by the referring courts in *eDate*,[135] *Pickney*,[136] and *Hejduk*,[137] recommended by AG Jääskinen in *Pickney*,[138] and is advocated by many authors.[139] It is also used by national courts in both the EU[140] and the US[141].

Targeting gives effect to the idea that most internet activity is not actually aimed at a worldwide audience but is merely the most effective way to reach certain audiences or pursue certain business models.[142] Thus, it is argued, information society service providers should not be subject to the jurisdiction of the courts or the substantive laws of every country in which their online content is accessible but only to the legal systems of those countries that they have actively targeted.

Such 'targeting' may be established in two ways. The orthodox understanding is to focus on the defendant's *subjective* intention to address an audience in a certain jurisdiction as it is 'manifested' by objective criteria such as the language of a publication or the currency with which one may pay. This seems to be the form of targeting test that the ECJ developed in *Pammer*,[143] *L'Oréal*,[144] and *Football Dataco*,[145] and that AG Jääskinen advocated in *Pickney*[146]; it is also used by some national courts applying Article 7(2) Brussels Ia in the area of unfair competition.[147] Alternatively, one may focus on the actual content in question and the jurisdictions to which it is *objectively* connected. This form of targeting seems to be used by the ECJ in the area of data protection[148] and was proposed by AG Cruz Villalón in *eDate* as a second element of the proposed criterion of the 'centre

[133] See *Football Dataco* (n 130) [39] (on Directive 96/9); Case C-324/09 *L'Oréal* [2011] ECR I-6011, [64] (on Directive 89/104/EEC and Regulation 40/94). See also Cases C-5/11 *Donner* ECLI:EU:C:2012:370, [28]–[29] (on the Information Society Directive) and Joined Cases C-446/09 and C-459/09 *Philips and Nokia* [2011] ECR I-12469 (on Regulation 40/94 and others) regarding offline infringements and Case C-98/13 *Blomqvist* ECLI:EU:C:2014:55 (on Directive 2001/29/EC, Directive 2008/95/EC, and Regulation 207/2009) concerning actual delivery to customers in the EU. See also S Depreeuw and J-B Hubin, 'Of Availability, Targeting and Accessibility: Online Copyright Infringements and Jurisdiction in the EU' (2014) 9 JIPLPract 750, 753–6.

[134] *Pammer* (n 23).

[135] *eDate* (n 17) [24].

[136] *Pickney* (n 25) [15].

[137] *Hejduk* (n 22) [14].

[138] AG Jääskinen, Opinion on *Pinckney* (n 50) [63]–[66].

[139] See, eg, Lein (n 34) [4.113]; Reymond (n 38) 415–45; Savin (n 15) 59; Schulz (n 3) 816–19.

[140] See, eg, Cass, Ch com, 20 Mar 2012, No 11.10-600 (French Court of Cassation, commercial chamber); BGH 12 Dec 2013, RIW 2014, 377, [24]; 2 March 2010, *New York Times* (n 43) [20]; 25 Oct 2011, BGHZ 191, 219, [11]. See also Martón (n 6) 211–13.

[141] See, eg, *Cybersell v Cybersell* 130 F 3d 414 (9th Cir 1997) 419–20; *CompuServe v Patterson*, 89 F 3d 1257 (6th Cir 1996). It is based on the 'effects test' developed in *Calder v Jones* 465 US 783 (US SCt 1984). See also Wang (n 3) 70–73; Jiminez and Lodder (n 5) 276.

[142] See section III.A.

[143] *Pammer* (n 23) [75]–[91]. See Martón (n 6) 213–14; Bogdan (n 5) 7; Svantesson (n 119) 301–3.

[144] *L'Oréal* (n 134) [64]–[66].

[145] *Football Dataco* (n 131) [39].

[146] AG Jääskinen, Opinion on *Pinckney* (n 50) [64], [66].

[147] Cass, Ch com, 20 Mar 2012 (n 141); BGH 12 Dec 2013 (n 141) [24]; 30 Mar 2006, *Arzneimittelwerbung im Internet*, IPRax 2007, 446, [21].

[148] *VKI* (n 106) [81]; Case C-230/14 *Weltimmo* ECLI:EU:C:2015:639, [32], [41] (focusing on an objective connection between the establishment and the jurisdiction in question).

of gravity of the dispute'.[149] It is also used by national courts to establish jurisdiction for personality right violations[150] and has been proposed by a number of authors, including those of the recently published *Geneva Internet Disputes Resolution Policies*,[151] as an alternative to the subjective targeting test.[152]

A number of strong arguments can be advanced in favour of both of these targeting tests, and in particular the one developed in *Pammer*. First and foremost, it seems to strike a sensible balance between the interests of the parties: while the provider of an information society service that is directed at an audience in a certain State can hardly complain about the jurisdiction of the courts of this State and the application of its substantive laws, potential claimants can reasonably expect to have access to these courts and to be able to rely on the laws of this State.[153] It thus allows service providers to better calculate the legal risk attached to their activities and to take measures to avoid certain jurisdictions. Second, targeting tests generally enhance legal certainty, provided that they are based on factors that are easy to assess. Third, such tests align well with the principle of proximity as they vest jurisdiction in the courts, and render applicable the laws, of a State that is supposed to have a close connection to the case in question.[154]

Still, there are a number of objections that can be raised to the targeting test used in *Pammer*. First, it does not have any concentrating effect where information society services actively (or inadvertently)[155] target a global audience.[156] Second, the room that it leaves to service providers to influence jurisdiction and applicable laws may be seen as an invitation to manipulate the relevant factors, especially where they are enumerated in a predefined list of criteria[157] that can easily be circumvented.[158] Third, it may also incentivize geo-blocking, a form of targeting strongly opposed by the EU Commission (as far as it concerns the internal market).[159]

4. *Country of origin*

The fourth criterion that would allow for a concentration of jurisdiction and applicable law is the country of origin. It currently only applies, in a limited

[149] AG Cruz Villalón, Opinion on *eDate* (n 48) [62]. See Martón (n 6) 215–16.
[150] BGH 2 March 2010, *New York Times* (n 43) [20]; 25 Oct 2011 (n 141) [11].
[151] Université de Genève, 'Geneva Internet Dispute Resolution Policies 1.0' (December 2016) <https://geneva-internet-disputes.ch/medias/2016/11/gidrp-1-0-geneva-internet-dispute-resolution-policies-final.pdf>.
[152] Reymond (n 38) 217–21; Svantesson (n 3) 365–8; Lutzi (n 122) 813.
[153] Schulz (n 3) 818.
[154] Depreeuw and Hubin (n 133) 764.
[155] Which may be the case for many services that use the English language and do not otherwise geographically restrict their audience.
[156] Briggs (n 130) [4.163]; Mills (n 64) 24; Bollée and Haftel (n 38) 1292; Gössl (n 3) 282.
[157] See, eg, *Pammer* (n 23) [80]–[84].
[158] Reymond (n 38) 213; Thünken (n 50) 936.
[159] Section III.A.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

number of cases, to the question of choice of law by virtue of Article 3(2) e-Commerce Directive.[160] It is closely linked to primary EU law and the free movement of persons[161] (but not itself a general principle of EU law)[162] and strongly favoured by the EU Commission as a way to reduce the number of applicable laws in internet cases.[163]

Within the scope of application of the e-Commerce Directive, Article 3(2) effectively limits the applicable laws to the national law of the information society service provider's country of establishment. According to recital (19) of the directive, a service provider is 'established' in the country where they pursue 'an economic activity through a fixed establishment for an indefinite period'; if they have several establishments in this sense, the place from where the service in question is provided is decisive. The definition in recital (19) not only has a strong similarity to the one used in recital (22) General Data Protection Regulation, it also resembles the criterion of the 'habitual residence' in Regulations Rome I and II and, in particular, the criterion of a 'branch, agency or other establishment' in Article 19(2) Rome I, Article 23 (1) Rome II, and Article 7(5) Brussels Ia as interpreted in *Somafer*.[164]

A similar provision does not presently exist at the level of jurisdiction. However, the default rule under Brussels Ia is the *actor sequitur forum rei* principle in Article 4(1), according to which a defendant domiciled in the EU can always be sued in their country of domicile. In practice, this will often be identical to the defendant's establishment as defined in the e-Commerce Directive.[165] In addition, the country-of-origin principle as formulated in the Directive also aligns with a number of other provisions of Brussels I, including Article 7(1)(b) second indent (as interpreted in *Wood Floor*),[166] the causal-event limb of Article 7(2) (as interpreted in *eDate* and *Wintersteiger*),[167] Article 7(5), and Article 8(1).

From a regulatory perspective, a country-of-origin approach undeniably presents some important advantages. It has the potential to greatly reduce the numbers of available jurisdictions and applicable laws and to significantly enhance legal certainty by focusing on an element that usually is easy to identify for both the parties[168] and the national courts.[169] Moreover, it would

[160] For other substantive EU instruments using a similar approach, see art 2(1), 3(1) 4(6) Dir 2010/13/EU; Art 2(1), 2a(1), 3(6) Dir 89/552/EEC as amended by Dir 2007/65/EC; Art 2 Dir 93/83/EEC.

[161] Höning (n 15) 3–9; J Basedow, 'Kohärenz im Internationalen Privat- und Verfahrensrecht der Europäischen Union' in J von Hein and G Rühl (eds), *Kohärenz im Internationalen Privat- und Verfahrensrecht der Europäischen Union* (Mohr Siebeck 2016) 3, 20–1.

[162] See H-P Mansel, 'Anerkennung als Grundprinzip des Europäischen Rechtsraums' (2006) 70 RabelsZ 651, 673. See also Case C-233/94 *Germany v European Parliament* [1997] ECR I-2441, [64].

[163] See, eg, EU Digital Single Market Strategy (n 120) 5.

[164] Case 33/78 *Somafer* [1978] ECR 2183, [12]: 'a place of business which has the appearance of permanency'.

[165] See Martón (n 6) 238–39.

[166] *Wood Floor* (n 93) [42].

[167] *eDate* (n 17) [42]–[43]; *Wintersteiger* (n 22) [37]. See above, at n 22.

[168] Bigos (n 3) 590; Beall (n 127) 374–82, 88–90; Svantesson (n 109) 349–50. See also Briggs (n 130) [3.156].

[169] Thünken (n 50) 934.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

reflect the indivisibility of most internet activity[170] and incentivize further market integration and substantive harmonization within the EU.[171]

As with most rules advancing legal certainty, the main disadvantage of a country-of-origin approach is that it seems to undermine the principle of proximity, which is reflected by connecting factors such as the place of contract performance or the place of the damage.[172] By extension, such an approach would also significantly reduce the level of protection awarded to potential claimants. Although the ECJ does not understand the grounds for special jurisdiction as designed to afford stronger protection to a weaker party,[173] this risk is particularly important at the level of jurisdiction where a country-of-origin approach would confine a potential claimant to the courts in the defendant's home country. In a case concerned with a television broadcast (originating in the UK), the European Court of Human Rights recently even considered the non-availability of the courts in the claimant's home country despite the programme's obvious connection to it as a violation of Article 6(1) ECHR.[174] By the same token, a country-of-origin approach at the level of choice of law would deprive the claimant from relying on the laws of the country of their habitual residence.

In addition, the country-of-origin principle is regularly criticized for being easily manipulated[175] and for provoking a regulatory race to the bottom between the Member States.[176] In the way that it currently operates under the e-Commerce Directive, it also is very burdensome for the national courts, which need to draw a comparison between the regulatory burden imposed on the provider of an information society service by the substantive law determined by general choice-of-law rules and the law of its country of establishment.[177]

E. Possible Forms of Regulation

These different connecting factors could be given effect in a number of ways.

So far, the EU legislator has largely relied on general, technology-neutral rules of private international law.[178] This is due to the concern that rules

[170] Höning (n 15) 30; Thünken (n 50) 935.
[171] Thünken (n 50) 932–3.
[172] See Höning (n 15) 49–51.
[173] See above, at n 49.
[174] *Arlewin v Sweden* App No 22302/10 (ECtHR 1 March 2016) [72]–[73]. The decision was based on the Court's finding that the Swedish jurisdiction was not barred by the country-of-origin principle in art 2(1) Dir 2010/13/EU; the Court left open whether its decision would have been different if it were (ibid [64]).
[175] Gössl (n 3) 277–8.
[176] Höning (n 15) 30–1, 52–4; Kohl (n 3) 179; H Muir Watt, 'The Role of the Conflict of Laws in European Private Law' in Twigg-Flesner (n 125) 44, 56; Schulz (n 3) 811; Thünken (n 50) 930. It should be noted, though, that this form of regulatory competition arguably is a necessary consequence of the four freedoms of primary EU law and thus generally encouraged by both the ECJ (see its seminal decisions in Cases C-341/05 *Laval* [2007] ECR I-11767 and C-438/05 *Viking* [2007] ECR I-I-10779) and the Commission).
[177] Thünken (n 50) 929–30.
[178] See section I. The most prominent example for a technology-specific rule is art 3 e-Commerce Directive (which, however, does not operate as a traditional conflict-of-laws rule (see above, at n 17); Art 25(2) Brussels Ia is another rare example; the EU Parliament's proposition for a choice-of-law rule for defamation (European Parliament Resolution of 10 May 2012, 2009/2170 (INI)) would have been another one, had it been adopted.

aimed at a specific technology will inevitably become obsolete or inappropriate as technology advances, which often happens at a much greater speed than the law can possibly be reformed. In addition, technology-specific rules have the disadvantage of requiring an often difficult delimitation of their scope of application in light of a wide range of technologies that may or may not fall under them.[179]

Technology-neutral rules, on the other hand, may not always yield appropriate results. But instead of formulating new, technology-specific rules, one may also try to remedy this problem by a technology-specific interpretation of the existing rules, as the ECJ has demonstrated, admittedly with mixed success, in *Pammer* and *eDate*. This may include the refusal to apply a general rule where it simply cannot be given any sensible effect in light of a certain technology.[180]

Such an approach will be developed in the following section of this article. As the EU Commission seems to focus more and more on consolidation rather than extension of the existing rules of private international law,[181] it has the additional advantage of not requiring extensive intervention by the European legislator.

IV. PROPOSAL FOR AN ALTERNATIVE APPROACH

The following proposition will focus on the situation in which the provider of an information society service[182] is sued as this is where the current *status quo* has been found wanting.[183] As far as claims brought by a service provider (other than for a negative declaration)[184] are concerned, on the other hand, there seems to be little reason not to apply the regular rules on jurisdiction and choice of law. The proposed approach will be limited to service providers established in the EU as only they are affected by Articles 7–23 Brussels Ia and would be subject to a potential amendment of the e-Commerce Directive.[185]

The proposition does not apply to cases in which the parties have exercised their autonomy to select the competent court or the applicable law. This choice would still take precedence under Article 25 Brussels Ia, Article 3 Rome I, and Article 14 Rome II.

The proposed approach will first be outlined (A.) and then be tested against the facts of some of the cases that form the *status quo* (B.).

[179] Bigos (n 3) 603.

[180] As was proposed, albeit unsuccessfully, by AG Cruz Villalón in his opinion on *Hejduk* (n 37) [41]; see in more detail section IV.A.1; see also Haibach (n 89) 261 fn 21; Briggs (n 130) [4.242].

[181] See EU Justice Agenda for 2020, COM(2014), 144 final, 5–7.

[182] As defined at n 20.

[183] See section II.C.

[184] Which are subject to the same rules as an action that would try to engage their liability (*Folien Fischer* (n 50) [52]–[53]) and therefore to the same criticism.

[185] As to which see section IV.A.2.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

A. The Proposed Approach

In light of the respective strengths and weaknesses of the aforementioned methods of concentration, it has been argued that a coherent private international law approach to internet cases must consist of a combination of them.[186]

In the following, such a combination will be proposed. It will be argued that the country-of-origin principle should be combined with the targeting approach in order to create a coherent framework for internet cases that increases legal certainty and limits liability risks but also leads to fair solutions in individual cases and balances out the different interests of the parties. It will thus provide an opportunity to reconcile the difficulties caused by the ubiquity and virtuality of internet communication with the central paradigms of EU private international law.

It is submitted that this approach can be implemented, in principle, at both levels, jurisdiction and choice of law. Its benefits will presumably be greater in the area of jurisdiction, where the *status quo* is particularly unsatisfactory and where the proposed approach could be implemented with relatively little need for new legislation (1.); but it will also provide helpful guidance for potential reform at the level of choice of law (2.).

1. Jurisdiction

While the shortcomings of the *status quo* in the area of jurisdiction are obvious, it may seem hard to address them without relying on an overarching instrument like the e-Commerce Directive. It will be shown, though, that the proposed combination of a country-of-origin principle (a.) and a limited number of exceptions based on targeting (b.) requires relatively little change to the existing rules and can largely be achieved via their re-interpretation in light of the unique features of online communication.

a) General rule: Country of origin

It has already been established that a country-of-origin approach generally provides a number of important advantages.[187] If it were implemented at the level of jurisdiction, it would considerably enhance legal certainty by reducing the number of available fora and by making it easy to predict where a potential lawsuit would be adjudicated.

As mentioned before,[188] this approach would align well with the existing default mechanism under the Brussels Ia Regulation. According to Article 4 (1), jurisdiction is generally vested in the courts at the defendant's domicile, which, in practice, will regularly be the country of origin of the activity

[186] Bollée and Haftel (n 38) 1292. [187] See section III.D.4. [188] ibid.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

complained of.[189] Where the activity originated from the defendant's branch or establishment in a different country, though, the causal-event limb of Article 7 (2) (as interpreted in *eDate* and *Wintersteiger*)[190] and Article 7(5) allow a potential claimant to sue in the courts of this country instead.

In practice, this mechanism is, of course, regularly displaced by the alternative fora available under Article 7(1) and the place-of-the-damage limb of Article 7(2). Yet, it has been shown that the connecting factors used in these provisions are particularly difficult to apply to internet cases. The ubiquity and virtuality of internet communication have led to a multiplication of the places to which they refer. As a consequence, they have become increasingly difficult to predict and often have only the most tenuous connection to the dispute. Thus, one might argue that the aims of proximity and legal certainty that the Brussels Ia Regulation seeks to achieve[191] would be better served if instead of trying to identify a physical 'place of the damage' or 'place of contract performance', one would just fall back to Article 4(1), the causal-event limb of Article 7(2), and Article 7(5) Brussels Ia and limit jurisdiction for claims against information society service providers to the courts of their respective home countries.

The argument not to apply the special grounds for jurisdiction provided in Article 7(1) and (2) Brussels Ia where the relevant connecting factors are excessively difficult or even impossible to determine receives support from three cases in which the ECJ was confronted with exactly this problem.

In the first of these cases, *Réunion Européenne*,[192] goods had been shipped from Australia to the Netherlands and then further to France, where it was discovered that they had been damaged. Regarding the insurer's claim in tort brought against the initial carrier, the Court held that in such a case, the place of the causal event would be 'difficult or indeed impossible to determine'.[193] Consequently, the insurer could only rely on the place-of-the-damage limb of what is now Article 7(2) Brussels Ia.[194]

In the second case, *Besix*,[195] the Court was asked to determine the place of performance of an exclusivity and non-competition clause, which it considered to be 'applicable in any place whatever in the world'.[196] It held that,

> [i]t follows from [the principle of legal certainty] that [Article 7(1) Brussels Ia] is to be interpreted as meaning that, in the event that the relevant contractual obligation has been, or is to be, performed in a number of places, jurisdiction to hear and determine the case cannot be conferred on the court within whose jurisdiction any one of those places of performance happens to be located.[197]

Conferring jurisdiction to the courts in any Member State that could be considered a place of performance would 'not avoid a multiplicity of competent courts'[198] and

[189] See Wang (n 3) 45–7.
[190] *eDate* (n 17) [42]–[43]; *Wintersteiger* (n 22) [37]. See also *Shevill* (n 24) [24]; *Hejduk* (n 22) [25]; and above, (n 23).
[191] See recital (16).
[192] Case C-51/97 [1998] ECR I-06511.
[193] ibid [33].
[194] ibid.
[195] *Besix* (n 54).
[196] ibid [20].
[197] ibid [28].
[198] ibid [34].

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

> [involve] the risk that the claimant will be able to choose the place of performance which he judges to be most favourable to his interests.
>
> Consequently, that interpretation does not make it possible to identify the court most qualified territorially to determine the case. Furthermore, it is likely to reduce the predictability of the competent court, so that it is incompatible with the principle of legal certainty.[199]

Therefore,

> it appears that [Article 7(1) Brussels Ia] is not apt to apply in a case […] where it is not possible to determine the court having the closest connection with the case. […][200]
>
> [J]urisdiction can, in such a case, be determined solely in accordance with [Article 4(1) Brussels Ia], which provides a certain and reliable criterion.[201]

Both decisions were primarily based on the principle of legal certainty, which mandates a narrow interpretation of the exceptions to the general *actor sequitur forum* rule of Article 4(1) Brussels Ia[202] and their exclusion in cases where they cannot be applied with sufficient certainty.

Finally, in *Hejduk*,[203] the ECJ was confronted with a similar problem in an internet case regarding the infringement of copyrights on the defendant's website that could be accessed from all Member States. In his opinion, AG Cruz Villalón followed the Portuguese government and the European Commission[204] in arguing that in case of such a 'delocalized' damage,

> the best option is to exclude the possibility of suing in the courts of the State where the damage occurred and to limit jurisdiction, at least that which is based on [Article 7(2) Brussels Ia], to that of the courts of the State where the event giving rise to the damage occurred.[205]

Considering it 'not possible to apply the criterion of the place where the damage occurred' in such a case,[206] he proposed to exclude it as a potential ground for jurisdiction and refer the claimant to the courts in the place of the causal act and in the defendant's domicile.[207]

In each of these cases, one of the connecting factors from Article 7(1) and (2) Brussels Ia was disapplied because the nature of the case made it impossible to locate them with the necessary degree of certainty. In *Besix* and the AG's opinion on *Hejduk*, this (would have) limited jurisdiction to the defendant's domicile,[208] which will regularly be the country of origin of the activity complained of.[209]

[199] ibid [34]–[35]. [200] ibid [48]. [201] ibid [50]. [202] ibid [26], [52]–[54].
[203] *Hejduk* (n 22). [204] See AG Cruz Villalón, Opinion on *Hejduk* (n 37) [19], [20].
[205] ibid [45]. [206] ibid [41].
[207] ibid [45]. A similar argument was made in an offline case by AG Jääskinen, Opinion on Case C-352/13 *CDC*, [47]–[53]; it remained equally unheard.
[208] In *Hejduk*, this followed from an overlap between art 4(1) and the causal-event limb of art 7(2) Brussels Ia, see ibid [45]. [209] See above, at n 189.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

Although the AG's proposition in *Hejduk* was evidently not followed by the ECJ, it is argued that the reasoning behind it could be applied to internet cases more generally, considering that they regularly give rise to a difficulty in localizing the places referred to in Article 7(1) and (2).[210] Instead of bending and twisting the interpretation of these provisions until they can be applied to internet cases, the approach used in the aforementioned cases (and *Besix* in particular) would allow the courts to disregard these provisions altogether where their application would lead to results that cannot be justified by the considerations that underlie them. Instead, one would naturally fall back to criteria that do not raise these difficulties—the place of acting in Article 7 (2),[211] the place of establishment in Article 7(5), or the domicile of the defendant.[212] To borrow a metaphor from two authors writing generally about jurisdiction for internet cases,[213] the appropriate approach may not consist in searching for the competent court in 'the high seas', but rather at the 'harbours' of internet communication.[214]

As the defendant's domicile will regularly be identical to their establishment as defined in the e-Commerce Directive,[215] the proposed approach would also increase the consistency between the areas of jurisdiction and choice of law, at least within the scope of application of the Directive. In many cases, Article 4 (1), the causal-event limb of Article 7(2), and Article 7(5) Brussels Ia would confer jurisdiction to the courts of the country to which Article 3(2) of the Directive refers in order to determine the applicable regulatory standard.

Admittedly, adopting the proposed approach would require the ECJ to overrule some well-established case law. Given that it has refused to do so even when a similar solution was proposed by AG Cruz Villalón in *Hejduk*, such a change may, in practice, be unlikely to occur without legislative intervention.[216] Still, the fact that the proposed approach could theoretically be achieved through a mere reinterpretation of the existing rules of Brussels I exempts it from one of the most pertinent points of criticism levelled against the country-of-origin principle in the e-Commerce Directive: the difficulty of differentiating between online and offline cases. By acknowledging that the grounds for special jurisdiction provided in Article 7(1) and (2) should not be applied where an internet case is simply too tenuously connected to any of the places to which they refer, the proposed approach would allow for a high degree of flexibility in addressing different situations to which internet communication gives rise on a case-by-case basis.

[210] For a similar argument see A Dickinson, 'By Royal Appointment: No Closer to an EU Private International Law Settlement?' (24 October 2012) <http://conflictoflaws.net/2012/by-royal-appointment-no-closer-to-an-eu-private-international-law-settlement/>.

[211] See Bigos (n 3) 604–9 [212] See above, at n 168. [213] Jiménez and Lodder (n 5).

[214] ibid 268–70. For a similar argument see Briggs (n 130) [3.156].

[215] See section IVA.1.a.

[216] An opportunity for which may arrive when the Regulation is revisited in 2022 (see art 79).

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

b) Exception for consumer cases: Targeting

The main argument that can be advanced against a country-of-origin approach is that it would undermine the principle of proximity underlying the grounds for special jurisdiction. Thus, it seems to reduce the level of protection of potential claimants.[217] Indeed, while the approach proposed above appears as a useful default rule, it is liable to create injustice where it is applied to asymmetrical relationships between a strong and a weak party. Requiring a company to sue another one for an alleged copyright infringement at the latter's place of business may be justifiable, even if this place is the other side of the European Union; requiring an individual artist to do so hardly is.

Against this backdrop, it appears justified to make an exception to the country-of-origin approach for structurally weaker parties. Of course, such an exception already exists for consumer contracts, for which Article 18(1) provides an additional forum at the consumer's domicile, provided that the professional's activity was directed at this Member State.[218] This exception is not only in line with the e-Commerce Directive,[219] Article 6(1) Rome I, and the high level of protection of the fundamental rights of EU citizens in EU private international law,[220] but it has also provided the ECJ with an opportunity to develop a (subjective) targeting test that strikes a reasonable balance between the need for legal certainty and the adequate protection of the weaker party.[221]

Although the ECJ, following its decision in *Brogsitter*,[222] seems to apply an increasingly wide interpretation to the protective rules on jurisdiction in Article 10–23 Brussels Ia that also includes certain claims in tort,[223] extending Article 17 to all cases involving consumers will most certainly require a textual change.[224] But there are not many arguments against it. As a matter of principle, consumers merit the same level of protection whether their relationship to a structurally stronger party is contractual or not.

The ECJ developed a definition of the term 'consumers' in *Benincasa*. It focused on the transaction in question, requiring the contract to have been concluded 'for the purpose of satisfying an individual's own needs in terms of private consumption'.[225] This definition can be modified so that it also covers non-contractual situations: a consumer, in this sense, is everyone who acts privately and with regard to their own needs, as opposed to someone acting in pursuit of a professional activity. While this definition evidently

[217] See section III.D.4.

[218] In addition, art 18(2) limits the fora where the consumer can be sued to their home jurisdiction; this coincides with the country-of-origin approach, though.

[219] Art 3(3) e-Commerce Directive and Annex, 6th indent. See also Thünken (n 50) 932, 935.

[220] See E Crawford and J Carruthers, 'Connection and Coherence between and among European Instruments in the Private International Law of Obligations' (2014) 63 ICLQ 1, 19–20.

[221] See section III.D.3. See also Stone (n 32) 14–15.

[222] Case C-548/12 *Brogsitter* ECLI:EU:C:2014:148, [25]–[27].

[223] See Case C-47/14 *Holterman* ECLI:EU:C:2015:57, [67]–[71]. See also *Alfa Laval v Separator Spares* [2012] EWCA Civ 1569, [24]–[33]; OGH 11 Aug 2015, IPRax 2017, 105.

[224] See AG Cruz Villalón, Opinion on *Hejduk* (n 37) [31].

[225] *Benincasa* (n 79) [17].

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

leaves room for a number of grey areas, these would be largely similar to those that already exist under the definition presently applied to Article 17 Brussels Ia.[226]

A definition along the lines of *Benincasa* may, however, be problematic when it comes to violations of reputation and privacy. Even where these rights are primarily or even exclusively affected with regard to a professional activity, they always concern a person in their private sphere as well. Just as personality rights cannot be meaningfully sliced up into territorial portions, they cannot easily be divided into a professional and a private sphere. It is therefore proposed to generally consider violations of a natural person's personality rights as consumer cases for the purpose of the proposed exception.

It is evident, though, that the jurisdictional protection of Articles 18 and 19 cannot be awarded to a party acting on their own behalf for the sole reason that they are structurally weaker than someone acting professionally; this would entirely undermine the legal certainty that is gained for information society service providers from the proposed country-of-origin approach. Thus, in addition and as a safeguard, it should be required that the activity complained of is pursued in or directed at the Member State where the consumer is domiciled. If parties acting in relation to their profession want to exclude the risk of being hauled to a court in Member States different from their place of establishment by a structurally weaker party, they will have to make sure that their activity does not target audiences in these places.[227]

Deciding whether a certain Member State has been targeted may be more difficult in situations not involving consumer contracts as the criteria developed with regard to Article 17 Brussels Ia can only be used by analogy. Yet, it will often be possible to establish that an activity is directed at individuals in a certain Member State even if it is not aimed at the conclusion of a contract—just as it can be difficult to establish a sufficient degree of targeting where it is.[228]

Inspiration for this determination in non-contractual cases could be taken from the ECJ's case law regarding the substantive scope of certain instruments on IP law that also require targeting.[229] Further guidance may be found in the new General Data Protection Regulation, which makes its application dependent on whether the activities of a data controller or processor are related to 'the offering of goods or services, irrespective of

[226] See Briggs (n 130) [4.115]–[4.157].

[227] Which admittedly raises the question of how such forms of dis-targeting can be reconciled with the proposed geo-blocking Regulation (n 121); see J von Hein, 'Geo-Blocking and the Conflict of Laws: Ships That Pass in the Night?' (31 May 2016) <http://conflictoflaws.net/2016/geo-blocking-and-the-conflict-of-laws-ships-that-pass-in-the-night/>).

[228] See Lutzi (n 90) 2071.

[229] See above, at n 133.

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

whether a payment of the data subject is required, to […] data subjects in the Union'.[230]

2. Applicable Law

Generally speaking, the proposed combination of a country-of-origin principle and a targeting approach seems equally suitable to replace the mosaic approach at the level of the applicable law. In fact, the country-of-origin approach already applies in the areas of personality right violations, unfair competition,[231] and contract law[232] thanks to the e-Commerce Directive; for consumer contracts, it is even balanced out by an exception that relies on a targeting test.[233] However, in its present form, the country-of-origin principle does not operate as a choice-of-law rule but only as a substantive corrective.[234]

This raises two principal questions with regard to the proposed approach. First, should the country-of-origin principle be reformulated as a proper choice-of-law rule? Second, should its scope be extended to also cover, in particular, IP right violations?

Regarding the first question, it is true that the country-of-origin principle in its present form enhances legal certainty only to a limited degree. It still requires the courts to first determine the applicable law according to the relevant choice-of-law rules and then to draw a comparison between the regulatory burden imposed by this law and the laws in place in the information society service provider's home country in order to determine whether the former constitutes a restriction of 'the freedom to provide information society services from another Member State'. This imposes a considerable burden on the courts and makes it hard for a potential claimant to foresee on which laws they may rely. Thus, legal certainty is mainly increased for the service provider, who ultimately needs to comply only with the laws at their place of establishment.

This problem would be solved if the country-of-origin principle operated as a proper choice-of-law rule for internet cases that referred to the law of the service provider's country of establishment.[235]

Such a rule could either be implemented via a textual modification of Article 3(2) e-Commerce Directive[236] or by adding a new provision for internet cases to

[230] Art 3(2)(a) GDPR. Where the Regulation applies, however, the claimant will enjoy the jurisdictional privilege under Art 79(2) regardless of his particular Member State having been targeted.

[231] With the exception of cartel law, see art 1(5)(c) e-Commerce Directive.

[232] With the exception of the freedom to choose the applicable law and consumer contracts, see art 3(3) e-Commerce Directive and Annex, 5th and 6th indent.

[233] Art 3(3) e-Commerce Directive, Annex, 6th indent, and art 6 Rome I.

[234] See above, at n 17.

[235] See Thünken (n 50) 940–41. Interestingly, such a rule would be relatively similar to the one proposed by the European Parliament to include personality rights violations in the Rome II Regulation (n 179), which also focuses primarily on the defendant and their activity, rather than on the claimant and the damage they purport to have suffered.

[236] Which would evidently also require deletion of recital (23) and art 1(4). During the negotiations of the Rome II Regulation, it was argued that a regulation would be preferable to a

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

Regulations Rome I and II. The former approach presents a number of advantages. First, it would require a textual change only to an instrument that deals specifically with online activity but leaves the general rules of EU private international law untouched. The rule would derive its scope of application directly from the e-Commerce Directive; it would use the same definition of information service society providers established in the EU, be subject to the same exceptions[237] and not be restricted by the limitations of Regulations Rome I and II, which do not cover, for instance, violations of privacy and personality rights.

If the rule were implemented, on the other hand, by adding a new provision to Regulations Rome I and II, this would raise a further difficulty. While the e-Commerce Directive only applies to information society service providers established in the EU, the provisions in the Rome Regulations are generally of universal application. As many information society service providers are established outside of the EU, a general country-of-origin rule would thus regularly refer to the laws of non-Member States. Even though the provisions on overriding mandatory rules[238] and public policy[239] would still act as safeguards, such a rule would come at a significant risk of undermining the high level of protection that EU citizens enjoy under the laws of the Member States. It would also go considerably beyond the main policy consideration underlying the e-Commerce Directive, ie to ensure free movement of information society service providers within the EU.

Of course, even if the rule were implemented via Regulations Rome I and II, it could still be limited to service providers established in EU Member States. Yet, while such a limitation would not be entirely unprecedented,[240] it would be rather difficult to reconcile with the many universal provisions in the Rome Regulations. Instead, it seems preferable to implement the proposed rule via a reformulated Article 3(2) e-Commerce Directive, which would take precedence over the general rules in the Rome Regulations by virtue of Article 23 Rome I and Article 27 Rome II.

As to its wording, the reformulated provision should consist of two parts. In its first part, it should refer to the law of the information society service provider's country of establishment for all private law actions that fall within the 'coordinated field' of the e-Commerce Directive as defined in its Article 2 (h). In its second part, it should make an exception that allows consumers (as

directive when implementing uniform choice-of-law rules (see Proposal for a Regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (Rome II), COM(2003) 427, 7); of course, this does not exclude the possibility of introducing such a rule via a directive; besides, it is not unlikely that a reformed e-Commerce Directive would take the shape of a regulation (similarly to the recent reform of EU data protection law).

[237] Most importantly, it would preserve the parties' freedom to choose the applicable law (art 3(3) e-Commerce Directive and Annex, 5th indent), which should, however, be extended to non-contractual situations. Regarding the exception for consumer contracts (Annex, 6th indent), see below.

[238] Art 9 Rome I; art 16 Rome II.

[239] Art 21 Rome I; art 26 Rome II.

[240] See eg art 3(4), 7(1) Rome I; art 14(3) Rome II.

defined above)[241] to rely on the laws of their own country of domicile, provided that this country has been targeted by the service provider's activity in question. While a similar exception already applies to consumer contracts pursuant to Article 6 Rome I, including it in the proposed rule would not only increase its visibility, it would also solve the problem of how to extend it to non-contractual obligations.

As to the rule's scope of application, Article 3(2) e-Commerce Directive currently covers all areas discussed above, with the exception of IP right violations.[242] This raises the question of a potential extension to this area. The proposed rule would indubitably be particularly beneficial to legal certainty in the area of IP law,[243] which is currently subject to an unmitigated mosaic approach (via the *lex loci protectionis* rule of Article 8(1) Rome II).

However, the adherence to this approach is widely seen as a direct consequence of the territoriality of IP rights,[244] which has repeatedly been emphasized by the ECJ.[245] Thus, it may be more sensible to address the unwelcome effects of the mosaic theory in the area of IP rights only at the level of jurisdiction. Regarding the applicable law, they seem bound to decrease anyway, at least within the EU, considering the Commission's commitment to further harmonize the Member States' substantive IP laws.[246]

B. Application to Selected ECJ Cases

In order to illustrate how the proposed approach would improve the present framework of EU private international law with regard to internet cases, it will be applied to the facts of three seminal decisions by the ECJ. Although they each involve parties from the same two countries, they illustrate a wide range of private law actions related to internet activity.

1. eDate

In *eDate*,[247] a German domiciliary sued an Austrian internet portal in Germany to force it to refrain from making available online certain information regarding a criminal conviction of his. The ECJ held that what is now Article 7(2) Brussels Ia would confer jurisdiction in such a case not only to the courts of the publisher's place of establishment[248] and every State where the material

[241] See section IV.A.1.b.
[242] Pursuant to art 3(3) e-Commerce Directive and Annex, 1st indent.
[243] See Mazziotti (n 118) 374. See also Green Paper on the online distribution of audiovisual works in the European Union, COM(2011) 427 final, 12–13, which discusses an extension of the country-of-origin approach.
[244] See eg R Fentiman 'Choice of Law and Intellectual Property' in J Drexl and A Kur (eds), *Intellectual Property and Private International Law* (Hart 2005) 129, 137–41.
[245] *Hejduk* (n 23) [22]; *Pinckney* (n 25) [39]. See AG Jääskinen, Opinion on *Pinckney* (n 50) [44]–[50]; Bogdan (n 5) 199.
[246] See EU Digital Single Market Strategy (n 120) 6–8.
[247] *eDate* (n 17).
[248] ibid [42].

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

could be accessed (in respect of damage caused in that territory)[249] but also to the courts of the claimant's centre of interests;[250] under Article 3(2) of the e-Commerce Directive, the competent courts would be free to determine the applicable law according to their own choice-of-law rules, but had to make sure that the defendant would not be 'made subject to stricter requirements than those provided for by the substantive law [of the service provider's home country]'. The German courts subsequently assumed jurisdiction as the courts of the claimant's centre of interests;[251] yet, the claim was unfounded under the applicable German law, so that no comparison had to be drawn with the law of the Austrian information society service provider's country of establishment.[252]

According to the approach proposed here, however, Article 7(2) Brussels Ia would not apply insofar as it points to the place of the damage or the claimant's centre of interests, neither of which could be reconciled with the principles of proximity and legal certainty in cases of internet publication; instead, Article 4 (1) and the causal-event limb of Article 7(2) would both confer jurisdiction to the Austrian courts as the courts of the defendant's domicile and establishment. As the claimant was, however, concerned as a private person (and claims against violation of privacy are proposed to be generally considered as consumer cases),[253] they would be able to rely on the exception made for structurally weaker parties in an extended Article 18, provided that it could be established that the defendant online portal had targeted their activity at a German audience.

Thus, the proposed approach would most likely not affect the jurisdiction of the German courts in the present case. However, it would change its justification from Germany merely being the claimant's centre of interests to the aim of protecting a structurally weaker party via a jurisdictional privilege. The decision in *eDate* may also have been informed by the Court's wish to award better protection to the claimant,[254] but this consideration is only indirectly reflected by the centre-of-interests criterion it developed.

Regarding the applicable law, a reformulated Article 3(2) e-Commerce Directive would in principle refer to Austrian law but allow the claimant consumer to rely on German law. Although this different approach would not affect the outcome of the present case, it would make a difference if German law provided a remedy since the proposed provision would not refer to Austrian law as a substantive corrective.

[249] ibid [51].
[250] ibid [48].
[251] BGH 8 May 2012, *rainbow.at II*, IPRax 2013, 252, [18].
[252] ibid [30].
[253] See section IV.A.1.b. Thus, the claim in *Martinez*, which was somewhat related to the claimant's career as an actor, would also have fallen under the exception.
[254] See *eDate* (n 17) [47], and the Opinion of AG Cruz Villalón (n 48) [48].

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

2. Hejduk

In *Hejduk*,[255] an Austrian photographer sued a German entity in Austria to recover damage caused by them having made available some of her photos on their homepage without authorization. The ECJ held that jurisdiction would be vested both in the courts of the country where the material was uploaded (for the entirety of the damage) and in the courts of every State where it could be accessed (for the damage caused by the infringement of national IP law through such access), including Austria.[256] While the Court was not asked to determine the applicable law, Article 8(1) Rome II would have referred to the substantive law of Austria as this was the country for which protection was sought.

According to the approach proposed here, however, the Austrian courts would not have jurisdiction under the damage limb of Article 7(2) Brussels Ia; instead, jurisdiction could only be based on its causal-act limb and the general rule in Article 4(1), both of which would point to the courts of Germany. As the claimant was clearly concerned in a professional capacity, there would be no room for a targeting-based exception. While this may seem unfair on the potential victim of an IP right infringement, it is justified by the absence of a structurally weaker party. Besides, it only leads to the application of the general *actor sequitur forum rei* rule of Article 4(1), the perceived unfairness of which is arguably better addressed via a procedural privilege than via the mosaic approach, which indiscriminately shifts the procedural burden entirely upon the defendant.

The question of the applicable law, on the other hand, would remain unaffected by the approach advocated here since it maintains the exception for IP rights in the e-Commerce Directive. Thus, while the claimant would be required to bring their action in Germany, they could still rely on Austrian law to claim protection for the Austrian territory.

3. Pammer

In *Pammer*,[257] an Austrian domiciliary seized the Austrian courts to seek compensation from a German shipping company in relation to a voyage that he had booked through the homepage of an intermediary company. The ECJ provided a non-exhaustive list of factors which would allow the determination of whether the defendant had directed their activity, via the intermediary, to consumers in Austria,[258] conferring jurisdiction to the Austrian courts under Article 18 Brussels Ia and (presumably) rendering Austrian law applicable under Article 6 Rome I (absent a choice of law).

Given that both of these rules would remain unaffected by the changes proposed here, the outcome of the case would be the same in the event that

[255] *Hejduk* (n 22). [256] ibid [24], [34]. [257] *Pammer* (n 24). [258] ibid [76]–[84].

https://doi.org/10.1017/S0020589317000240 Published online by Cambridge University Press

the service provider's activity had been directed at the consumer's Member State. But even if it had not (and the consumer contract provisions did not apply), the result would be the same as under the present framework. First, because there would be no reason to disapply Article 7(1) Brussels Ia in the present case: while identifying the place of contract performance may be difficult in the case of a voyage that spans a number of countries,[259] it is certainly not impossible;[260] besides, this difficulty has nothing to do with the contract being concluded on the internet. Second, because the proposed country-of-origin rule for choice of law would point to the same substantive law as Article 4(1)(b) Rome I, which refers to the service provider's habitual residence.

V. CONCLUSION

This article has critically discussed how the general rules of EU private international law address the particular difficulties of internet cases. It started with the observation that the two distinctive features of internet communication are its ubiquity and virtuality, which lead to a multiplication of increasingly tenuous connections to physical places in internet cases.

When applying the rules of EU private international law to internet cases, the ECJ has repeatedly allowed jurisdiction and the application of substantive laws to be based, at least for a territorially limited part of the action, on these tenuous connections, following the so-called mosaic approach; in addition, it has created an additional ground of jurisdiction for online violations of personality rights at the claimant's centre of interests. It has been shown that both of these approaches, although somewhat balanced at the level of choice of law by Article 3(2) e-Commerce Directive, generally give an undue advantage to the potential claimants in internet cases. They also conflict with several paradigms of EU private international law, including the principles of legal certainty (because they make it hard to foresee for potential defendants where they may be sued), proximity (because jurisdiction and the applicable law can often be based on a very weak connection to a Member State), and the sound administration of justice (because they create a risk of multiple lawsuits over small parts of an overall action).

Based on these observations, an alternative approach to claims against information society service providers established in the EU has been proposed. It has been argued that a combination of the country-of-origin principle and a targeting-based exception in the style of Article 18 Brussels Ia and Article 6 Rome I would increase legal certainty and the jurisdictional

[259] See Case C-533/15 *Frisman* OJ C 48, 8 Feb 2016, 8, which the ECJ will unfortunately not get an opportunity to decide.

[260] Guidance could be found in Cases *Wood Floor* (n 93); C-204/08 *Rehder* [2009] ECR I-6073; *Color Drack* (n 93).

protection of potential defendants while preserving the current high standard of protection for claimants who act in pursuit of their private interests.

It has been shown that such an approach could be implemented at the level of jurisdiction via a reinterpretation of Article 7(1) and (2) Brussels Ia along the lines of the ECJ's decision in *Besix* but would require a textual change to Article 17(1) in order to extend it to non-contractual situations. Regarding the applicable law, the reformulation of Article 3(2) e-Commerce Directive is proposed so that it acts as a traditional choice-of-law rule, which would generally refer claims against information society service providers to their respective country of establishment; but again, an exception should be made for claimants who are acting as private persons in order to allow them to rely on their home laws, provided that the country of their habitual residence has been targeted.

By applying this approach to a selection of ECJ cases, it has been shown that the proposed approach, while not necessarily changing the outcome of these cases, would provide a stronger theoretical foundation for their resolution, which would be more faithful to both the particularities of internet communication and the central paradigms of EU private international law.